PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-110225
(43)Date of publication of application : 21.04.2005

(51)Int.CI. H04L 9/32
G06F 17/60

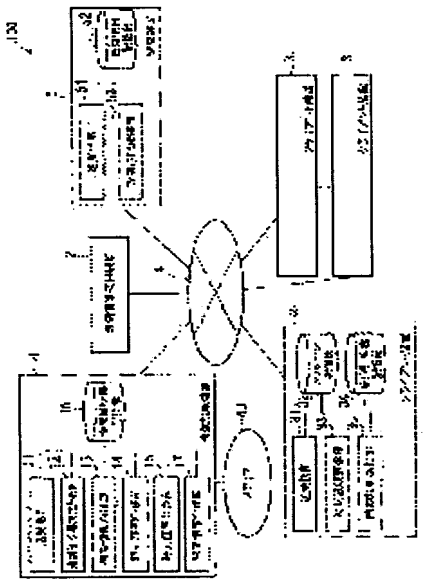
(21)Application number : 2004-256035
(22)Date of filing : 02.09.2004

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HOTTA HIDEKAZU
ONO SATOSHI
TAKURA AKIRA

(30)Priority
Priority number : 2003315701 Priority date : 08.09.2003 Priority country : JP

(54) TIME CERTIFICATION METHOD, TIME CERTIFICATION AUDIT METHOD, TIME CERTIFICATION DEVICE, AUDIT DEVICE, TIME CERTIFICATION PROGRAM, TIME CERTIFICATION AUDIT PROGRAM, TIME CERTIFICATION VERIFICATION PROGRAM, AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To simply verify an acceptance certification with a user's device, and at the same time, verify the acceptance certification without using public information periodically published to media, etc., and verify the trueness of time given to the acceptance certification.
SOLUTION: A time stamp system 100 comprises a time certification device 1, a time information offering device 2 which offers time information used for the creation of the time stamp, a plurality of client devices 3i, an audit device 5 which performs the audit of the acceptance certification issued by the time certification device 1, and a computer network 4 which mutually connect the respective devices. The time certification device 1 replies the acceptance certification to the client device 3i responding to the time certification request from the client device 3i, and at the same time, if doubt arises in the acceptance certification, the client device 3i can verify the acceptance certification by the information published to media, etc. 40 by the time certification device 1, or the audit result by the audit device 5.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-110225
(P2005-110225A)
(43)公開日　平成17年4月21日(2005.4.21)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/32	H04L	9/00	675Z	5J104
G06F 17/60	G06F	17/60	140	
	H04L	9/00	675D	

審査請求 未請求　請求項の数 49　OL　（全 121 頁）

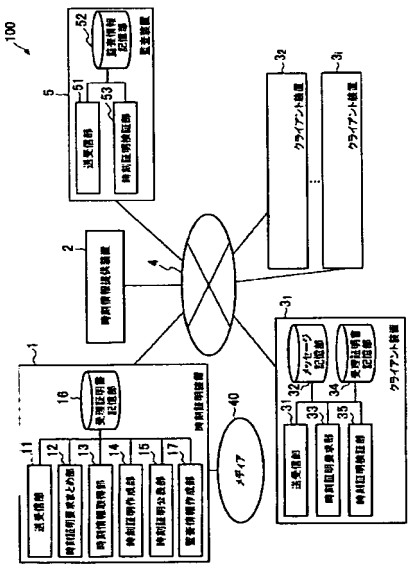
(21)出願番号　特願2004-256035 (P2004-256035)
(22)出願日　平成16年9月2日 (2004.9.2)
(31)優先権主張番号　特願2003-315701 (P2003-315701)
(32)優先日　平成15年9月8日 (2003.9.8)
(33)優先権主張国　日本国(JP)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100083806
弁理士　三好　秀和
(72)発明者　堀田　英一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　田倉　昭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Fターム(参考)　5J104 AA11　MA01　PA07

(54)【発明の名称】時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体

(57)【要約】
【課題】　利用者装置で簡単に受理証明書の検証ができるとともに、定期的にメディア等へ公表する公表情報を用いなくても受理証明書の検証を行うことができ、かつ、受理証明書に付された時刻の真正性を検証することができる。
【解決手段】　タイムスタンプ・システム100は、時刻証明装置1、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、複数のクライアント装置3ｉ、時刻証明装置1が発行した受理証明書の監査を行う監査装置5、及び以上の各装置を相互に接続する、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置3ｉからの時刻証明要求に応えて、受理証明書をクライアント装置3ｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置3ｉは時刻証明装置1がメディア等40に公表した情報、又は、監査装置5による監査結果によって受理証明書を検証することができる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、
前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、
予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、
前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、
複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、
前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、
前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、
前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、
前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得ステップと、
前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、
前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信ステップと、
前記第２のルート値を前記公表機関に公表する公表ステップと、
前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、
を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情

報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項２】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記第２のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び

前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項３】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信ステップと、

前記第２のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利

用者装置に送信する第２の補完情報送信ステップと、
を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項４】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記第２のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、
を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項５】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、
を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項６】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項３乃至５のいずれか１項に記載の時刻証明方法。

【請求項７】

前記第１の時刻証明要求まとめステップは、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成ステップは、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項１乃至６のいずれか１項に記載の時刻証明方法。

【請求項８】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査ステップと、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査ステップと、
前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、
前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、
を有することを特徴とする時刻証明監査方法。
【請求項９】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、
予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、
前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、
前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査ステップと、
前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第１のルート値に一致するか否かにより、前記受理証明書を検証する第２の監査ステップと、
前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、
前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有することを特徴とする時刻証明監査方法。

【請求項１０】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１１】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連す

る情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１２】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まと

め手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１３】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記

単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１４】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木

のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査ステップと、

前記第１の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、

前記第１の監査ステップ、前記第２の監査ステップ、及び前記第３の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１５】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まと

め手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査ステップと、

前記第１の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第２の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、

前記第１の監査ステップ、前記第２の監査ステップ、及び前記第３の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１６】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法に

より、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項１７】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項１２乃至１６のいずれか１項に記載の時刻証明監査方法。

【請求項１８】

前記第１の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項８乃至１７のいずれか１項に記載の時刻証明監査方法。

【請求項１９】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割

り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、

前記第２のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項２０】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記第２のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項２１】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に

割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、

前記第２のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項２２】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手

段と、
前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、
予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、
前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、
複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、
前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、
前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、
前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、
前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、
前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、
前記第２のルート値を前記公表機関に公表する公表手段と、
前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、
を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。
【請求項２３】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、
前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手

段と、
前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、
予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、
前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、
前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、
前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、
前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、
前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、
前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、
を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。
【請求項２４】
前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項２１乃至２３のいずれか１項に記載の時刻証明装置。
【請求項２５】
前記第１の時刻証明要求まとめ手段は、
前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、
前記受理証明書作成手段は、
前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項１９乃至２４のいずれか１項に記載の時刻証明装置。
【請求項２６】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査手段と、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

を有することを特徴とする監査装置。

【請求項２７】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二

分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査手段と、

前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第１のルート値に一致するか否かにより、前記受理証明書を検証する第２の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

を有することを特徴とする監査装置。

【請求項２８】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフか

ら前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする監査装置。

【請求項２９】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書

を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする監査装置。

【請求項３０】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記

補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする監査装置。

【請求項３１】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻

及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする監査装置。

【請求項３２】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査手段と、

前記第１の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には

、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、
前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、
前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査手段と、
前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、
前記第１の監査手段、前記第２の監査手段、及び前記第３の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、
を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする監査装置。
【請求項３３】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、
前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、
を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、
前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査手段と、

前記第１の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第２の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、

前記第１の監査手段、前記第２の監査手段、及び前記第３の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする監査装置。

【請求項３４】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、

を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする監査装置。

【請求項３５】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監

査装置を選択することを特徴とする請求項３０乃至３４のいずれか１項に記載の監査装置。

【請求項３６】

前記第１の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項２６乃至３５のいずれか１項に記載の監査装置。

【請求項３７】

請求項１乃至７に記載の時刻証明方法の各ステップを前記時刻証明装置に実行させることを特徴とする時刻証明プログラム。

【請求項３８】

請求項８乃至１８に記載の時刻証明監査方法の各ステップを前記監査装置に実行させることを特徴とする時刻証明監査プログラム。

【請求項３９】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と

、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、

前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する検証結果受信ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４０】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する監査結果受信ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４１】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信

ステップと、
前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、
前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、
前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、
前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第１の検証ステップと、
前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、
前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、
前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、
前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、
を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。
【請求項４２】
所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、
予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第１の検証ステップと、

前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４３】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報

を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第１の検証ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４４】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置

情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第１の検証ステップと、

前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４５】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて

、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、

前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、

前記保証書に含まれる前記デジタル署名の署名検証を行う第１の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第２の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４６】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木の

リーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受信ステップと、

前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、

前記保証書に含まれる前記デジタル署名の署名検証を行う第１の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、

前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第２の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４７】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証する検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項４８】

前記第１の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項３９乃至４７のいずれか１項に記載の時刻証明検証プログラム。

【請求項４９】

請求項３７乃至４８のいずれか１項に記載されたプログラムを記録していることを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、所定のデジタル情報に時刻情報を付与するタイムスタンプ・システムに関し、より詳しくは、該タイムスタンプ・システムにおける時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体に関する。

【背景技術】

【０００２】
タイムスタンプ技術は、デジタルデータがある特定時刻に存在していることを証明するとともに、その時刻以降データが変更されていないことを証明する技術である。近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、交信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、時刻情報の付与、改ざんの検知、電子文書保管等の機能を具備するものであるが、タイムスタンプ技術は、このうち、時刻情報の付与及び改ざんの検知の機能を実現するものである。
【０００３】
図35は、このようなタイムスタンプ技術を用いたタイムスタンプ・システムを説明する図である。同図に示すタイムスタンプ・システム900は、利用者（要求者、検証者）30がタイムスタンプの対象データをＴＳＡ（Time Stamping Authority；タイムスタンプ生成機関）10に送信すると、ＴＳＡ10がＴＡ（Time Authority；時刻源である時刻情報提供機関）20から時刻情報を入手して、利用者30から要求された対象データに対してタイムスタンプを付した受理証明書を生成し、該受理証明書を利用者に返信するようになっている。そして、ＴＳＡ10で発行された受理証明書は、ＰＫＩ（Public Key Infrastructure；公開鍵基盤）のもとでデジタル署名を主要な偽造防止／証明手段として採用する場合には、一般に、利用者30から送られた対象データに時刻情報を付したデジタル署名を含んだ受理証明書となっている。
【０００４】
この受理証明書の真正性の主要な根拠としてデジタル署名を用いるタイムスタンプ・システムに関しては、ＴＳＡ10の不正、受理証明書の有効期間、およびシステム運用の面などにおいて問題点が指摘されている。そのため、受理証明書の真正性の主要な根拠としてデジタル署名を用いないタイムスタンプの方法も提案されている。例えば、線形リンキング（Linear Linking Protocol）による方法（例えば、特許文献1および特許文献2参照。）は、ＴＳＡ10が仮に信頼できないとしてもシステム全体として高い安全性を確保することが可能となっている方法である。図36は、ＰＫＩに依存しない線形リンキングによるタイムスタンプ・システムを説明する図である。同図に示すタイムスタンプ・システム910は、複数の利用者30のタイムスタンプ対象データ（ハッシュ値）を相互に関連付けるリンク情報Ｌｎを生成し、リンク情報Ｌｎに時刻を付したタイムスタンプを返信するようになっており、各タイムスタンプが、それまでに生成されたすべてのタイムスタンプに依存するようになっている。そして、このリンク情報の一部（ＬＭ、ＬＮ）が定期的にメディア等（例えば新聞）に公表されるので、これにより、ＴＳＡ10の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。
【特許文献１】特許第3278721号明細書
【特許文献２】特許第3281881号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上述した線形リンキングによるタイムスタンプの方法に関しては、利用者30が利用する利用者装置で受理証明書の検証を行うには、膨大な計算処理が必要となり、検証が容易でないという課題がある。例えば、時刻証明を毎秒間隔で行い、1週間に1回メディア等（例えば新聞）に公表するタイムスタンプ・システムの場合、利用者30は、最大約60万個（60×60×24×7）のリンク情報をＴＳＡ10からもらって計算しなければならないこととなる。
【０００６】
また、リンク情報を1回メディア等（例えば新聞）に公表してから、次の公表までの間においては、利用者30はＴＳＡ10で発行された受理証明書を検証することができないという課題がある。即ち、ＴＳＡ10が一旦1回メディア等（例えば新聞）にリンク情報を公表した後には、受理証明書を偽造することは不可能であるが、リンク情報の公表と次の公表

までの間においては、受理証明書を偽造することは原理的に可能であるため、この期間にＴＳＡ10が不正をしていないという検証が必要となっても、検証をすることができない。

【０００７】

さらに、上述したデジタル署名を受理証明書の真正性証明の主要手段とする方法、および線形リンキングによるタイムスタンプにおいては、受理証明書に付された時刻の真正性についてTSA10 の誤動作や不正を検出する手段が与えられていないため、該時刻の真正性については全面的に TSA10を信頼する他に方法がないという課題がある。

【０００８】

本発明は、上記の課題を解決するためになされたものであり、デジタル署名を用いない、又はデジタル署名を主要な手段とはしないタイムスタンプ・システムにおいて、利用者装置で簡単に受理証明書の検証ができるとともに、定期的にメディア等へ公表する公表情報を用いなくても受理証明書の検証を行うことができ、かつ、受理証明書に付された時刻の真正性を検証することができる時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記目的を達成するため、請求項1記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の

補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信ステップと、前記第２のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００１０】

請求項２記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記第２のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明

書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００１１】

請求項３記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信ステップと、前記第２のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを要旨とする。

【００１２】
請求項４記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめステップと、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記第２のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００１３】
請求項５記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行

う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【００１４】

請求項６記載の本発明は、請求項３乃至５のいずれか１項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【００１５】

請求項７記載の本発明は、請求項１乃至６のいずれか１項に記載の発明において、前記第１の時刻証明要求まとめステップは、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成ステップは、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【００１６】

請求項８記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接

値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査ステップと、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有することを要旨とする。

【００１７】

請求項９記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後

、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査ステップと、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第１のルート値に一致するか否かにより、前記受理証明書を検証する第２の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有することを要旨とする。

【００１８】

請求項１０記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が

作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００１９】

請求項１１記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公

開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００２０】

請求項１２記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に

付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００２１】

請求項１３記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００２２】

請求項１４記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を

監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査ステップと、前記第１の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、前記第１の監査ステップ、前記第２の監査ステップ、及び前記第３の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【００２３】

請求項１５記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報

を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査ステップと、前記第１の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第２の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査ステップと、前記第１の監査ステップ、前記第２の監査ステップ、及び前記第３の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【００２４】

請求項１６記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装

置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【００２５】

請求項１７記載の本発明は、請求項１２乃至１６のいずれか１項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【００２６】

請求項１８記載の本発明は、請求項８乃至１７のいずれか１項に記載の発明において、前記第１の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【００２７】

請求項１９記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイ

ムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００２８】

請求項２０記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる

第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００２９】

請求項２１記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を

前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを要旨とする。

【００３０】

請求項２２記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１

のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【００３１】

請求項２３記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【００３２】

請求項２４記載の本発明は、請求項２１乃至２３のいずれか１項に記載の発明において

、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【００３３】

請求項２５記載の本発明は、請求項１９乃至２４のいずれか１項に記載の発明において、前記第１の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【００３４】

請求項２６記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置

が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査手段と、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有することを要旨とする。

【００３５】

請求項２７記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第１の監査手段と、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第１のルート値に一致するか否かにより、前記受理証明書を検証する第２の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有することを要旨とする。

【００３６】

請求項２８記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機

関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００３７】

請求項２９記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のル

ート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００３８】

請求項３０記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前

記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００３９】

請求項３１記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割

り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【００４０】

請求項３２記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後

付の補完情報の一部として送信する第１の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査手段と、前記第１の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第２の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、前記第１の監査手段、前記第２の監査手段、及び前記第３の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【００４１】

請求項３３記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報

受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第１の監査手段と、前記第１の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第２の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第３の監査手段と、前記第１の監査手段、前記第２の監査手段、及び前記第３の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【００４２】

請求項３４記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【００４３】

請求項３５記載の本発明は、請求項３０乃至３４のいずれか１項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監

査装置を選択することを要旨とする。

【００４４】

請求項３６記載の本発明は、請求項２６乃至３５のいずれか１項に記載の発明において、前記第１の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【００４５】

請求項３７記載の本発明は、請求項１乃至７に記載の時刻証明方法の各ステップを前記時刻証明装置に実行させる時刻証明プログラムであることを要旨とする。

【００４６】

請求項３８記載の本発明は、請求項８乃至１８に記載の時刻証明監査方法の各ステップを前記監査装置に実行させる時刻証明監査プログラムであることを要旨とする。

【００４７】

請求項３９記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステッ

プと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する検証結果受信ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００４８】

請求項４０記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる

前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する監査結果受信ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００４９】

請求項４１記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第１の検証ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステ

ップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５０】

請求項４２記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第１の検証ステップと、前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５１】

請求項４３記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第１の検証ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記時刻証

明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５２】

請求項４４記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否かを検証する第１の検証ステップと、前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第２の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記受理証明書および後付の補完情報から計算した前記第

２のルート値が一致するか否かを検証する第３の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５３】

請求項４５記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第１の補完情報受信ステップと、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、前記保証書に含まれる前記デジタル署名の署名検証を行う第１の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネット

ワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第２の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５４】

請求項４６記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第１のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第２の二分木において、前記計算方法により、前記要求から計算された前記第１のルート値を前記第２の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第２の二分木のルートに割り当てる第２のルート値を計算する第２の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第１の二分木のリーフから前記第２の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、該第１のルート値の前記第２の二分木における位置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第２のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受信ステップと、前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれる前記第２次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、前記保証書に含まれる前記デジタル署名の署名検証を行う第１の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第２の補完情報受信ステップと、前記公表機関から公表されている前記第２のルート値を取得する

公表機関利用ステップと、前記公表機関から取得した前記第２のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第２のルート値が一致するか否かを検証する第２の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５５】

請求項４７記載の発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を連接した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第１のルート値が、前記受理証明書に含まれる前記第１のルート値と一致するか否かに基づいて前記受理証明書を検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

【００５６】

請求項４８記載の発明は、請求項３９乃至４７のいずれか１項に記載の発明において、前記第１の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第１のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第１の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第１の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第２の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【００５７】

請求項４９記載の本発明は、請求項３３乃至４８のいずれか１項に記載されたプログラ

ムを記録しているプログラム記録媒体であることを要旨とする。

【発明の効果】

【００５８】

本発明によれば、デジタル署名を用いない、又はデジタル署名を主要な手段とはしないタイムスタンプ・システムにおいて、利用者装置で簡単に受理証明書の検証ができるとともに、定期的にメディア等へ公表する公表情報を用いなくても受理証明書の検証を行うことができ、かつ、受理証明書に付された時刻の真正性を検証することができる。

【００５９】

これにより、利用者は、大量のデータから膨大な計算処理を行わずに、受理証明書の検証をすることができる。また、時刻証明に関する情報がメディア等に公表されてから、次の公表までの間においても、受理証明書の検証を行うことができる。さらに、受理証明書に付された時刻についても検証をすることができる。

【発明を実施するための最良の形態】

【００６０】

以下、本発明の実施の形態を図面を用いて説明する。

【００６１】

＜第１の実施の形態＞

図1は、本発明の第１の実施の形態に係るタイムスタンプ・システム100のシステム構成図である。同図に示すタイムスタンプ・システム100は、ＴＳＡ10に設けられた時刻証明装置1、ＴＡ20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置3ｉ（ｉは自然数）、監視／監査機関に設けられ、時刻証明装置1が発行した受理証明書の監査を行う監査装置5、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置3ｉからのタイムスタンプ要求（時刻証明要求）に応えて、タイムスタンプつき受理証明書をクライアント装置3ｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置3ｉは、時刻証明装置1がメディア等40に公表した情報、又は、監査装置5による監査結果によって受理証明書を検証することができるようになっているコンピュータシステムである。

【００６２】

尚、上記コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【００６３】

時刻証明装置1は、コンピュータネットワーク4を介して時刻情報提供装置2、クライアント装置3ｉ、および監査装置5とデータを送受信する送受信部11、複数のクライアント装置3ｉからの時刻証明要求として送信されたメッセージ・ダイジェスト（デジタル・データから作成されるハッシュ値）を二分木を用いてまとめる時刻証明要求まとめ部12、受理証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部12でまとめられたメッセージ・ダイジェストに対して時刻情報取得部12で取得した時刻情報を付して受理証明書を作成する時刻証明作成部14、定期的にメディア等40に受理証明書に関する情報を公表する時刻証明公表部15、時刻証明作成部14で作成された受理証明書を記憶する受理証明書記憶部16、および監査装置5に送信する監査情報を作成する監査情報作成部17を具備している。

【００６４】

以下、時刻証明装置1の時刻証明要求まとめ部12、時刻証明作成部14、時刻証明公表部15、および監査情報作成部17の機能について、より詳しく説明する。

【００６５】

上述したように時刻証明要求まとめ部12は、二分木を用いて時刻証明要求をまとめるが、この二分木について図2および図3を用いて説明する。ここで、図2は、単位時間（例えば1秒、受理証明書を発行する時間間隔であり、この時間間隔をラウンドという。）に受

け付けた時刻証明要求を二分木のリーフに割り当てる値とする第１次二分木の一具体例を示す図であり、図3は、一定期間（例えば1週間、時刻証明装置1がメディア等40に受理証明書に関する情報を公表する公表サイクル）において第１次二分木のルート値をリーフに割り当てる値とする第２次二分木の一具体例を示す図である。

【００６６】

図2に示す第１次二分木は、予め定められた単位時間（上述したように例えば、1秒など）に1つ用意されるものであり、第１次二分木のリーフ（レベル0）には、ラウンド内に複数のクライアント装置3ｉから受け付けたメッセージ・ダイジェストを所定の手順に従って割り当てるようになっている。尚、第１次二分木の構成（高さ（レベルで表現する）、幅（番号で表現する））は、クライアント装置3ｉからの時刻証明要求の数に応じて変化するものであるため、本実施の形態における第１次二分木は動的に構成されるものであるが、以下においては、図2に示すように、16のリーフを有する第１次二分木の場合について説明し、動的な第１次二分木の構成に関しては、すべての実施の形態に共通の機能であるため、後述することとする。

【００６７】

第１次二分木の各ノード（リーフを除く）に割り当てられる値は以下のように計算する。第１次二分木の親の割当値は、左側の子の割当値H’と右側の子の割当値H”を連接（ビット列とビット列の結合）して、ハッシュ値を計算することにより求められるものであり、これをh(H’ ‖ H”）と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルート値）Hを求めると、該ルート値Hは、時刻証明作成部14において作成される受理証明書の一部である。

【００６８】

以後、第１次二分木のレベルj、番号iのノードをh(j,i)と表し、ルート値Hの算出方法を、図2を具体例に説明する。

【００６９】

あるクライアント装置3ｉから送信されたメッセージ・ダイジェストがh(0,5)であるとき、このリーフに割り当てられるハッシュ値h (0,5)からルート値H(＝h(4,0))を求めるには、h(0,5)にh(0,4)を左から連接して、ハッシュ値h1を計算し、該ハッシュ値h1にh(1,3)を右側から連接してハッシュ値h2を計算し、該ハッシュ値h2にh(2,0)を左側から連接してハッシュ値h3を計算し、さらに該ハッシュ値h3にh(3,1)を右側から連接してハッシュ値h4（＝H）を計算すればよい。即ち、H＝h(h(h(2,0)‖h(h(h(0,4)‖h(0,5))‖h(1,3)))‖h(3,1))である。ここで、例えば、h(0,4)を左（右）側から連接する場合を（L（R）,h(0,4)）のように表し、h(0,5)の値から二分木のルート値Hを計算するのに、必要なデータの集合を連接する方向、および連接する順序も含めて表すと、（（L, h(0,4)）、（R, h(1,3)）、（L, h(2,0)、（R, h(3,1)））となるが、以後、このデータの集合を、第１次二分木におけるh(0,5)の１次補完情報とよぶ。ここで、補完情報とは、二分木のルート値を計算するのに必要な自己の値以外のノード値の集合（ノードの位置情報も含む）をいい、第１次二分木における補完情報を１次補完情報、第２次二分木における補完情報を２次補完情報という。

【００７０】

このようにして、第１次二分木が構成され、ルート値 H が計算されと、次に各ラウンドで計算されたルート値Hをもとに第２次二分木が構成される。図3に示す第２次二分木は、予め定められた一定期間（上述したように例えば、1週間など）に1つ用意されるものであり、第２次二分木のリーフ（レベル0）には、第１次二分木のルート値 H を経時的に順次左側から割り当てるようになっている。尚、第１次二分木とは異なり、第２次二分木は固定的な構成となっているが（例えば、1ラウンドが1秒、公表サイクルが1週間の場合には、約60万個（60×60×24×7）のリーフを有する第２次二分木が構成される）、以下においては、図3に示すように、16のリーフを有する第２次二分木の場合について説明する。

【００７１】

第２次二分木の各ノード（リーフを除く）に割り当てられる値は、第１次二分木の計算方法と同じである。ここで、第２次二分木のレベルj、番号iのノードをM(j,i)と表して、図3に示す具体例を説明する。

【００７２】

今、第２次二分木のリーフに割り当てるハッシュ値がM(0,5)であるとき、このハッシュ値M(0,5)からルート値RH(＝M(4,0))を求めるには、M(0,5)にM(0,4)を左から連接して、ハッシュ値h1’を計算し、該ハッシュ値h1’にM(1,3)を右側から連接してハッシュ値h2’を計算し、該ハッシュ値h2’にM(2,0)を左側から連接してハッシュ値h3’を計算し、さらに該ハッシュ値h3’にM(3,1)を右側から連接してハッシュ値h4’（＝RH）を計算すればよい。そして、このルート値RHが、時刻証明公表部15を介してメディア等40に公表される公表情報である。また、第２次二分木におけるM(0,5)の補完情報（以下、２次補完情報という）は、（（L，M(0、4)）、（R，M(1,3)）、（L，M(2,0)）、（R，M(3,1)））となる。

【００７３】

時刻証明作成部14は、このようにして作成された第１次二分木のルート値H、第１次二分木のルート値Hの識別番号（第２次二分木のリーフを一意に特定できる番号）、それぞれのラウンドに付与される時刻（例えば、1秒間隔で付される）ｔ、１次補完情報 HK1、および２次補完情報 HK2 を含む受理証明書 TSC(H,t)を作成し、クライアント装置３ｉに送信するようになっている。尚、２次補完情報 HK2 に関しては、即時に取得できる２次補完情報（以後、即時２次補完情報という）と対象となる一定期間が終了後に取得できる２次補完情報（以後、後付２次補完情報という）の双方があるが、受理証明書 TSC(H,t)が作成される段階においては、即時２次補完情報だけが送信されるものであり、後付２次補完情報は、対象となる一定期間が終了後に送信されるものである。例えば、図3の具体例においては、M(0,5)にとって、M(2,0)、M(0,4)は即時２次補完情報であるが、M(1,3))、M(3,1)は後付２次補完情報である。

【００７４】

図4に受理証明書TSC(H,t)の構成を示す。尚、図4に示す受理証明書TSC(H,t)は、上述したようにクライアント装置3iから送付されたメッセージ・ダイジェストそのものを第１次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第１次二分木のリーフに割り付けてもよく、この場合には、図5に示すように受理証明書TSC(H,t)は、キー付ハッシュ関数を適用する際のハッシュ・キー κ も含む必要がある。より詳しくは、メッセージ・ダイジェストyを含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キー κ を決定し、κ をキーとして、yに対して、所定のキー付ハッシュ関数 h’を作用させ、ハッシュ値 h’(κ,y) を計算し、該ハッシュ値h’(κ,y)を第１次二分木のリーフに割り当てるもので、これにより、あるクライアント装置3iの送付したメッセージ・ダイジェストを他のクライアント装置3iに知られないようにすることが可能となる。

【００７５】

また、時刻証明作成部14は、クライアント装置３ｉから後付けの２次補完情報の要求があったときは、ある一定期間の途中であっても、その時点において取得できるとともに、まだ送信していない２次補完情報（以後、後付２次補完情報の一部という）を、オンライン補完証明書としてクライアント装置3iに送信するようになっている。

【００７６】

尚、時刻証明装置1から受理証明書TSC(H,t)をクライアント装置3iへの送信する際には、受理証明書TSC(H,t) の完全性の保証を高める補助手段として、時刻証明装置1が準備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけても送信するようにしてもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置3iからアクセス可能になっているものとする。

【００７７】

ここで、上記においては、受理証明書に付する時刻として、現在のラウンドに付与される時刻を用いたが、本発明はこれに限定されるものではなく、例えば、受理証明書に対し

て、以下に示す２つの時刻ｔ１及びｔ２を付し、当該の時刻証明要求が受け付けられた時刻が、時刻ｔ１より前でかつ時刻ｔ２より後であることを証明するような区間証明書にしてもよい。

【００７８】

図４６に、この場合の受理証明書の構成を示す。ここで、時刻ｔ１は、現在のラウンドの終結時刻とし、時刻ｔ２は、直前のラウンドの終結時刻である。そして、直前のラウンドの第１次二分木のルート値Ｈ’を現在の第１次二分木のリーフａ０への割当値とし、この直前のラウンドの第１次二分木のルート値Ｈ’と、リーフａ０の１次補完情報、即ち、リーフａ０の現在の第１次二分木における補完情報ＨＫ１’を受理証明書に含めるものである。

【００７９】

リーフａ０を現在の第１次二分木のどこに置くかについては、次の２つの方法がある。

【００８０】

第１の方法は、図４７に示すように、リーフａ０を現在のラウンドのルートの子ノードとして、現在の第１次二分木に含める方法である（リーフａ０のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは異なる）。

【００８１】

第２の方法は、図４８に示すように、リーフａ０を現在の第１次集約木のレベル０の一番左のリーフとする方法である（リーフａ０のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは同じである）。

【００８２】

尚、第１の方法は、第２の方法より、補完情報ＨＫ１’のデータ量が少なくて済むという効果がある（図４６に示す例においては、補完情報ＨＫ１’は、h(3, 0)のみ）。一方、第２の方法は、第１の方法より、実装上、第１次二分木を簡単に構成することができるという効果がある。

【００８３】

時刻証明公表部15は、時刻証明要求部12で作成された第２次二分木のルート値 RH を定期的（上述した一定期間ごと）にメディア等40に公表するものである。

【００８４】

監査情報作成部17は、監査情報を第２次二分木から取得して監査装置5に送信するものであり、より詳しくは、監査情報とは、第２次二分木のリーフに設けられた監視点に基づいて、監視点の１次情報（第１次二分木のあるリーフに割り当てられた情報およびその１次補完情報の組み合わせをいう）、監視点に割り当てられた第１次二分木のルート値H、該第１次二分木のルート値Hの識別番号、即時２次補完情報、および監視点に付与された時刻情報を意味する。図3に示す具体例によれば、M(0,10)が監視点となっているので、監査装置5に送信するデータは、M(0,10)の一次情報、M(3,0)、M(1,4) 、および M(0,10)に付与された時刻となる。

【００８５】

尚、図3の具体例においては、監視点は1つしか設けられていないが、所定のアルゴリズムに従って複数設けてよいのは勿論であり、また、監視点は時刻証明要求から作成されたルート値H が割り当てられたリーフ（図3の具体例においては、M(r;5)）より、右側のリーフ（時間的に後）に割り当てられていればどこに設けていてもよいものである。従って、時刻証明要求が割り当てられる第２次二分木のリーフの位置に依存せずに、監視点を有効に機能させるためには、第２次二分木の各リーフそれぞれを監視点とするのが好適である。

【００８６】

クライアント装置３ｉは、コンピュータネットワーク4を介して時刻証明装置1および監査装置5とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置1からの時刻証明要求に対する受理証明書TSC(H,t

)を記憶する受理証明書記憶部34、および受理証明書TSC(H,t)を検証する時刻証明検証部35を具備している。尚、時刻証明検証部35は、定期的にメディア等40に公表される公表情報を利用して検証を行う受理証明書に対する第１の検証機能と、メディア等公表前に監査装置5を利用して検証を行う受理証明書に対する第２の検証機能とを備えるものである。また、受理証明書が上述した区間証明書である場合には、時刻証明検証部35は、第１及び第２の検証に加えて、直前のラウンドの第１次二分木のルート値の検証を行う。これは、受理証明書に含まれる直前のラウンドの第１次二分木のルート値Ｈ’と該ルート値Ｈ’が割り当てられたリーフの１次補完情報ＨＫ１’から、現在のラウンドの第１次二分木のルート値を計算し、計算された該ルート値と受理証明書に含まれる第１次二分木のルート値が一致するか否かを検証するものである。

【００８７】

監査装置5は、コンピュータネットワーク4を介して時刻証明装置1およびクライアント装置３ｉとデータを送受信する送受信部51、時刻証明装置1から送信される監査情報を記憶する監査情報記憶部52、およびクライアント装置３ｉから受理証明書 TSC(H,t) の検証要求を受けた際には、クライアント装置３ｉから送信された検証要求情報および監査情報記憶部52に記憶されている監査情報を用いて受理証明書 TSC(H,t) の検証を行い、その結果をクライアント装置３ｉに返信する時刻証明検証部53を具備している。

【００８８】

ここで、時刻証明検証部53の機能について、図3の具体例を用いて説明する。図3の具体例においては、M(0,10)が監視点となっているので、この時点において監査装置5が受け取っている監査情報は、上述した通り、M(0,10)の１次情報、M(3,0)およびM(1,4)である。一方、クライアント装置３ｉは、検証要求情報として、M(0,5)の１次情報、２次補完情報としてM(0,4)、M(1,3)、およびM(2,0)を送信するものである。これは、クライアント装置３ｉが検証を求める時点（即ち、受理証明書 TSC(H,t) が発行されたM(0,5)の時点より後刻であるM(0,10)の時点）においては、即時２次補完情報に含まれていなかったM(1,3)も時刻証明装置1から取得することが可能であるので、M(1,3) をオンライン補完証明書として時刻証明検証要求者が時刻証明装置1から取得し、検証要求情報に含めたものである。

【００８９】

そして、時刻証明検証部53は、自己が有している監査情報 M(3,0) が、クライアント装置３ｉから送信された検証要求情報から計算された M(3,0) と一致するか否かを検証するものである。ここで、比較検証の対象となる第２次二分木のノード（図3の具体例においては、M(3,0)）を以後、認証点とよぶ。尚、一般に、クライアント装置３ｉから送信された時刻証明要求から作成されたルート値H が割り当てられた第２次二分木のリーフ（対象点とよぶ）の番号が監視点であるリーフの番号より小さい場合、認証点のラベルは監査情報に含まれており、また、監視点における時刻証明処理が終了した時点において、クライアント装置３ｉが受信できる１次情報および２次補完情報から作成されるラベルには、認証点のラベルが含まれるので、上記検証は常に実施可能なものであるが、この理由に関しては後述する。

【００９０】

また、時刻証明検証部53は、受信した監査情報に付された時刻および受理証明書 TSC(H,t)に付された時刻の真正性を検証する機能を有している。ここで、前者は、監査情報を受信した時刻（自己の参照する時計から取得）と監査情報に付された時刻の差が一定の限度内か否かを検証するものである。これに対して、後者は、前者の監査情報に付されている時刻が正しいときには、監査点に付与された時刻がわかるので、この監査点から受理証明書TSC(H,t)に付されるべき時刻を所定の単位時間間隔過去に遡ることにより算出し（例えば、図３に示す具体例においては、M(0,5) を含む受理証明書の検証要求を受けたとき、M(0,5) を含む受理証明書TSC(H,t)に付される時刻Ｔ１は、監査点に付与された時刻Ｔより、5単位時間間隔、過去にあるはずである）、該算出した時刻と受理証明書TSC(H,t)に実際に付された時刻の差が一定の限度内か否かを検証するものである。

【００９１】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（ＣＰＵ：Central Processing Unit）、プログラムやデータを収納する機能を有するＲＡＭ(Random Access Memory) 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置1の時刻証明要求まとめ部12、時刻情報取得部13、時刻証明作成部14、時刻証明公表部15および監査情報作成部17、クライアント装置3ｉの時刻証明要求部33および時刻証明検証部35、並びに監査装置5の時刻証明検証部53の処理は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、時刻証明装置1の受理証明書記憶部16、クライアント装置3ｉのメッセージ記憶部32および受理証明書記憶部34、並びに監査装置5の監査情報記憶部52は、上記主記憶装置の機能を備えたものである。

【００９２】

次に、以上の構成を有するタイムスタンプ・システム100における時刻証明方法、および時刻証明検証方法を図6乃至図9を用いて説明する。ここで、図6は、一公表サイクルにおいて時刻証明装置1が受理証明書 TSC(H,t) を作成する動作を説明するシーケンス図であり、図7は、監査装置5が監査情報の検証を行う動作を説明するフローチャートであり、図8および図9は、クライアント装置3iが受理証明書 TSC(H,t) の検証を行う動作を説明するフローチャートおよびシーケンス図である。

【００９３】

但し、ここで検証を行うクライアント装置3iを使用する利用者30は、検証の対象となる受理証明書TSC(H,t)を要求し取得した時刻証明要求者、及びこの時刻証明要求者から受理証明書TSC(H,t)を渡された時刻証明検証者の双方が考えられる。

【００９４】

まず、時刻証明方法について説明する。クライアント装置3i が時刻証明装置1にメッセージ・ダイジェストy を含む時刻証明要求を送信すると、時刻証明装置1は送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部12が、このメッセージ・ダイジェストyを第１次二分木のリーフに割り当てる（ステップＳ11, Ｓ12, Ｓ13）。そして、同一ラウンド内においては、複数のクライアント装置3iから受信した複数の時刻証明要求に対して、第１次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部12がそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第１次二分木のルート値Hを計算する（ステップＳ14, Ｓ15）。

【００９５】

次に、時刻証明要求まとめ部12が、第１次二分木のルート・ハッシュ値Hを第２次二分木のリーフに割り当てて、インクリメンタルに第２次二分木を構成していくとともに、時刻証明作成部14は、クライアント装置3iから送付されたメッセージ・ダイジェストy、第１次二分木のルート・ハッシュ値H、該ルート・ハッシュ値Hの識別番号n、時刻ｔ、１次補完情報HK1、および２次補完情報 HK2を含む受理証明書 TSC(H,t) を作成し、送受信部11を介してクライアント装置3iに受理証明書 TSC(H,t) を送信する（ステップＳ16, Ｓ17, Ｓ18）。

【００９６】

これにより、クライアント装置3iは、受理証明書 TSC(H,t) を取得することができる（ステップＳ19）。尚、受理証明書 TSC(H,t) に含まれる２次補完情報には、この時点において取得できる即時２次補完情報は含まれているが、後付２次補完情報は含まれていない。

【００９７】

次に、第１次二分木のルート値Hが割り当てられた第２次二分木のリーフが、監視点である場合には、監査情報作成部17が監査情報を作成し、この監査情報を送受信部11を介して監査装置5に送信する（ステップＳ20, Ｓ21, Ｓ22）。これにより、監査装置5は、監査情報を取得することができる（ステップＳ23）。ここで、監査装置5は、図7に示すように、監査情報に付与された時刻値のチェックを行う。これは、監査装置5が当該監査情報を受

信した時刻t1を自己が参照する時計から取得し、該時刻t1と、監査情報に付与された時刻時刻t' とを比較し、時刻差が、予め定められた限界値（例えば1秒）以内であれば、当該監査情報は時刻について正しいとみなすものである（ステップＳ301,S302,S303,S304）。尚、監査装置５が参照する時計は標準時にトレーサブルであることが望ましい。

【００９８】

そして、一定期間内においては、上述した時刻証明装置1の動作は繰り返され、一定期間が終了すると、時刻証明作成部14は、送受信部11を介して、クライアント装置３ｉに後付２次補完情報を含む補完証明書を送信する（ステップＳ24,Ｓ25）。これにより、クライアント装置３ｉは、受理証明書 TSC(H,t) とそのすべての２次補完情報を取得したことになる（ステップＳ26）。また、時刻証明公表部15は、第２次二分木のルート値 RH を計算し、このルート値 RH をメディア等40に公表する（ステップＳ27,Ｓ28）。

【００９９】

次に、メディア等40に公表された公表情報を用いた時刻証明検証方法について説明する。これは、クライアント装置３ｉの第１の検証機能に相当するものである。

【０１００】

まず、クライアント装置３ｉは、自己が時刻証明装置1に時刻証明要求として送信したメッセージ・ダイジェスト、並びに受信した受理証明書 TSC(H,t) 及び補完証明書に含まれている１次補完情報および２次補完情報（この時点においては、すべての２次補完情報を具備している）、から第２次二分木のルート値 RHcal を計算する（ステップＳ31）。

【０１０１】

次に、メディア等40に公表されている同一公表サイクルのルート値RHを取得し、このルート値RHが、計算したルート値RHcal に一致するか否か検証する（ステップＳ32,Ｓ33）。

【０１０２】

以上の検証において、検証に成功すれば、受理証明書 TSC(H,t) が改ざんされていないことを確認することができる（ステップＳ34）。一方、検証に失敗すれば、受理証明書 TSC(H,t) が改ざんされていることを確認することができる（ステップＳ35）。これにより、メディア等公表後においては、公表された情報を利用して、時刻証明装置1が発行した受理証明書 TSC(H,t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【０１０３】

次に、監査装置5を用いた時刻証明検証方法について説明する。これは、クライアント装置３ｉの第２の検証機能に相当するものである。

【０１０４】

まず、クライアント装置３ｉが、検証する時点における後付２次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップＳ41）。この要求を時刻証明装置1が送受信部11を介して受信すると、時刻証明作成部14は、後付２次補完情報の一部（この時点において取得できる後付２次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置３ｉに送信する（ステップＳ42,Ｓ43,Ｓ44）。これにより、クライアント装置３ｉは、オンライン補完証明書を取得するので、時刻証明検証部35は、これに既に受け取っている受理証明書TSC(H,t)（１次情報および即時２次補完情報、並びに受理証明書TSC(H,t)に付された時刻）を加えた検証要求情報を監査装置5に送信する（ステップＳ46）。

【０１０５】

次に、監査装置5が検証要求情報を送受信部51を介して受信すると、時刻証明検証部53は、この検証要求情報から認証点のラベル値Ａcal を計算する（ステップＳ47,Ｓ48）。一方、時刻証明検証部53は、監査情報として既に受け取っているこの認証点のラベル値Ａを監査情報記憶部52から取得して、この認証点のラベル値Ａが、計算により求めた認証点のラベル値Ａcal に一致するか否かを検証する（ステップＳ49）。そして、この検証に成功した場合には、受理証明書TSC(H,t)に付された時刻の真正性についても検証する（ステ

ップＳ50,S51）。これは監査情報に付された時刻から受理証明書TSC(H,t)に付されるべき時刻を算出し、該算出した時刻と受理証明書に付された時刻との差が一定時間内か否かを検証するものである。尚、受理証明書TSC(H,t)に付された時刻の真正性についての検証は、監査情報の時刻が正しいと検証された場合（ステップＳ303）を前提に行われるものである。

【０１０６】

以上の検証それぞれにおいて、検証に成功すれば、受理証明書TSC(H,t)が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップＳ52）。一方、いずれかの検証に失敗すれば、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップＳ53）。そして、時刻証明部53は、この検証結果を送受部51を介してクライアント装置3ｉに送信する（ステップS54,Ｓ55）これにより、メディア等公表前においても、時刻証明装置1が発行した受理証明書 TSC(H,t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【０１０７】

以上、第１の実施の形態のタイムスタンプ・システム100によれば、クライアント装置3ｉから時刻証明要求を受け付けた時刻証明装置1が、第１次二分木を用いて時刻証明要求をまとめ、このまとめた値に対して時刻情報を付した受理証明書TSC(H,t)を発行し、第２次二分木のルート値をメディア等40に公表するので、デジタル署名を用いない、又はデジタル署名を主要な手段としないタイムスタンプ・システムであっても、クライアント装置3ｉは公表情報および補完情報から簡単に受理証明書TSC(H,t)の検証をすることができる。また、第２次二分木のルート値をメディア等40に公表する前であっても、監査装置5が第２次二分木の監視点に関する監査情報を有しているので、監査装置5はクライアント装置3ｉからの検証要求を受けて、受理証明書TSC(H,t)の検証をすることができる。

【０１０８】

尚、第１の実施の形態のタイムスタンプ・システム100は、上述した形態に限定されるものではなく、受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、監査機関の選択方法、補完証明書の種類などについて種々のバリエーションを施すことが可能である。以下、このことについて説明する。

【０１０９】

まず、受理証明書に含まれる補完情報のパターンについて説明する。

【０１１０】

本実施の形態の受理証明書は、１次補完情報および即時２次補完情報を含める方式であったが、受理証明書に含める補完情報（以下、受理証明書内補完情報という。）については、以下に述べるような３つの方式の中から、状況に応じて利点のある方式を採用することができるものである。

【０１１１】

タイプ０の受理証明書内補完情報は、第１次二分木のルート値と、第１次二分木における補完情報（１次補完情報）のみを含むものとする。

【０１１２】

タイプ１の受理証明書内補完情報は、上記タイプ０の情報と、第２次二分木のルート値を計算するための補完情報（２次補完情報）を含むものとする（これは、上述した本実施の形態で採用された方式である）。

【０１１３】

タイプ２の受理証明書内補完情報は、公表間隔の中の、指定された時刻あるいは第１次二分木のルート値の識別番号以降に取得できる全ての第１次二分木のルート値（第２次二分木のリーフ値）を含むものとする。

【０１１４】

通常の状況においては、クライアント装置3iで第２の検証を行うためには、タイプ１の情報があれば十分である。また、タイプ０の受理証明書内補完情報を採用した場合におい

ては、時刻証明装置１が、タイプ１の情報に含まれタイプ０の情報には含まれない補完情報をクライアント装置3iの要求に応じて提供することにより、クライアント装置3iで第２の検証を行うことが可能である。

【０１１５】

上記のようにクライアント装置3iで第２の検証を行うためにはタイプ０の受理証明書内補完情報を採用することも可能であるが、タイプ１の受理証明書内補完情報を採用することにより、該公表期間内に、当該の受理証明書より前に発行された他の受理証明書とリンクする情報を取得できるという利点がある。この利点を生かす例としては、クライアント装置3iが、タイプ１の受理証明書内補完情報を取得することにより、必要ならば、図9における監査装置５の役割を実行することが可能となることが挙げられる。具体的には、あるクライアント装置3 aが時刻証明を要求したのがある時刻 t より前であることを、他のクライアント装置3 b が時刻証明装置1や監査装置５に頼ることなく検証することが以下のように可能となる。まず、クライアント装置3 bは、時刻 t において時刻証明装置1に対して時刻証明要求を送付し、それに対する受理証明書 TSC(H, t) を受信するものとする。但し、受理証明書 TSC(H, t) にはタイプ１の受理証明書内補完情報がふくまれているものとする。その後、クライアント装置3 bは、他のクライアント装置3 aに対して、クライアント装置3 aが受信した受理証明書TSC(H, t)とオンライン補完証明書を含む検証に必要なデータを自己に送付させ、さらにクライアント装置3 b は、図9における監査装置5の役割を実行するものである。そして、ステップS49 の判定で YES と判断されれば、時刻 t 以前にクライアント装置3 a が時刻証明要求をしたことが、他のクライアント装置3 bにより確認されるものである。

【０１１６】

これに対して、タイプ２の受理証明書内補完情報は、ある公表期間の途中で事故等によりTSA10のサービスが中止した場合でも、該公表期間内に、当該の受理証明書より前に発行された他の受理証明書とリンクする情報を取得できるという利点があるものである。

【０１１７】

第２次二分木を示す図3を参照して、タイプ２の受理証明書内補完情報について説明する。ここで、クライアント装置3iが受け取る第1次二分木のルート・ハッシュ値を M(0,5) とする。このとき、タイプ２の受理証明書内補完情報は、指定された識別番号が2 のとき、[M(0,2)、 M(0,3)、 M(0,4)]となる。そして、クライアント装置3 iは上記の受理証明書内補完情報を受信していれば、たとえTSA10が受理証明書受信後に破綻したとしても、受理証明書が正しいことを検証することができる（例えば、他のクライアント装置3iが受け取った第１次二分木のルート・ハッシュ値M(0,2)と、受理証明書に含まれたM(0,2)が一致すれば、自己の受理証明書が正しいことを検証できる）。

【０１１８】

ところで、クライアント装置3iにおいては、どのタイプの受理証明書内補完情報を受理証明書と同時に受信するかを、利用者30とTSA10との契約により指定することができる。尚、受理証明書内補完情報と補完証明書に含まれる補完情報は相関があるものであり、例えば、タイプ１又は２の受理証明書内補完情報を受信する契約をしている場合には、補完証明書として後付の２次補完情報を受信することになり、また、タイプ０の受理証明書内補完情報を受信する契約をしている場合には、補完証明書として２次補完情報すべてを受信することになる。また、契約とは別に、時刻証明要求時のオプションにより、受理証明書内補完情報を指定できるようにしてもよいものである。また、クライアント装置3iは、第２の検証を行うために、オンライン補完証明書を要求することができるものであるが、その際、タイプ１の受理証明書内補完情報を取得していた場合には、受理証明書発行以後に確定した２次補完情報を受信すればよいが、タイプ０の受理証明書内補完情報を取得していた場合には、その時点で確定している２次補完情報の全てを受信する必要がある。

【０１１９】

さらに、クライアント装置3iは、クライアント装置3iからの要求時にのみ補完証明書を受信するという契約（補完証明書を公表間隔終了時に受信しない）をしてもよいものであ

り、この場合には、２次補完情報は、直前に終了した公表間隔の間に発行された受理証明書の補完証明書のみではなく、さらに遡って過去に発行された受理証明書に対応する補完証明書を要求することも可能となるものである。

【０１２０】

ここで、一般にTSA10の提供する時刻証明サービスの契約者は、個人の場合もあるし組織／法人の場合も考えられるが、いずれにせよ、契約者が時刻証明サービスを使用する契約をする際には、アカウントが発行され、契約者はこのアカウントを用いて、時刻証明サービスを受けることになる。その際、パスワード等の認証用の情報が発行されるのが普通である。従って、各契約者は契約時に、その契約者のアカウントを用いて為された時刻証明要求に対する補完証明書の送付先を指定することができるが、これは、例えば、電子メールのアドレスなどの電子的手段の他、郵送の宛先など電子的でない手段もありえるものである。

【０１２１】

次に、上記補完証明書の種類について説明する。

【０１２２】

公表間隔の間に、ある契約者に対して発行される受理証明書は一般に複数あると考えられる。このような場合、契約者に対して送信されるデータ量の合計を考慮すると、複数の受理証明書に対する補完証明書のデータ構成は次の２つの種類が考えられる。以下において、N は公表間隔の間に計算する、第１次二分木のルート値の個数である。

【０１２３】

第１は、本実施の形態において説明した簡約型の補完証明書であり、公表用データである第２次二分木のルート値を再構成するのに必要な、最小限の補完情報を含めるものである（２次補完情報の個数は、各受理証明書に対して log2(N)。例えば、図３において、時刻証明要求の第１次二分木ルート値がM(0,5)の場合には、M(0,4) 、M(1,3) 、M(2,0) 、M(3,1)) 。第２は、列挙型の補完証明書であり、公表間隔の間に発行した受理証明書の第１次二分木のルート値を全て含めるものである（２次補完情報の個数はN。図３の場合においては、M(0,0)、M(0,1)、…、M(0,15)) 。

そして、契約者は契約時に、上記２つの種類の補完証明書のうち、どちらかを選択して指定できるようになっている。ここで、契約に際しては、１つの公開期間の間に、時刻証明サービスのある契約者が受領する受理証明書の数が、一定の限度より少ないときには簡約型の補完証明書の方がデータ量が小さいが、その限度を超えると列挙型の補完証明書の方がデータ量が小さくなるので、契約者は受領する受理証明書の数に応じて最適な方式を選択すればよい。

【０１２４】

尚、クライアント装置3iが、列挙型の補完証明書を用いて第１の検証を行う場合には、図8のステップＳ31 において列挙型の補完証明書に記載されている第１次二分木のルート値の識別番号、及び第１次二分木のルート値から、第２次二分木のルート値を計算する。

【０１２５】

次に、監査情報に含まれる補完情報のパターンについて説明する。

【０１２６】

本実施の形態の監査情報は、１次補完情報および即時２次補完情報を含める方式であったが、監査情報に含める補完情報（以下、監査情報内補完情報という。）については、以下に述べるような３つの方式の中から、状況に応じて利点のある方式を採用することができるものである。

【０１２７】

タイプ０の監査情報内補完情報は、監視点の１次情報（第１次二分木のあるリーフに割り当てられた情報およびその１次補完情報の組み合わせをいう）からなる。

【０１２８】

タイプ１の監査情報内補完情報は、上記タイプ０の情報と、第２次二分木のルート値を計算するための補完情報（２次補完情報）を含むものとする（これは、上述した本実施の

形態で採用された方式である）。

【０１２９】

タイプ２の受理証明書内補完情報は、公表間隔の中の、指定された時刻あるいは第１次二分木のルート値の識別番号以降に取得できる全ての第１次二分木のルート値（第２次二分木のリーフ値）を含むものとする。

【０１３０】

タイプ０の監査情報内補完情報を採用する場合、ある監査装置５は、自己の担当する監視点に属する受理証明書に対してのみ、クライアント装置3iからの時刻証明検証要求に応じることができる。これは、第２次二分木において監視点と時刻証明要求点が一致するのであれば、クライアント装置3iが受け取る受理証明書に含まれる受理証明書内補完情報と、監査装置５が受け取る監査情報内補完情報との一致を検証することにより、受理証明書の検証ができるからである。従って、任意の時刻証明検証要求にどれかの監視／監査機関が確実に応じるためには、全ての単位時間（すべての第２次二分木のリーフ）がなんらかの監視／監査機関の監視点となっている必要がある。

【０１３１】

通常の状況においては、公表期間の終了前にあるクライアント装置3iが受信した受理証明書の内容を監査装置5が受信した監査情報とリンクし、時刻証明検証を行うためには、タイプ１の情報があれば十分である。

【０１３２】

タイプ２の受理証明書内補完情報は、上述した受理証明書内補完情報の場合と同様に、通常の状況において時刻証明検証を行うためには必要ないが、ある公表期間の途中で事故等によりTSA10のサービスが中止した場合でも、該公表期間内に、当該の受理証明書より前に発行された受理証明書に対して時刻証明検証を行うことができるという利点があるものである。

【０１３３】

第２次二分木を示す図3を参照して、タイプ２の監査情報内補完情報について説明する。ここで、監査装置5が受け取る第1次二分木のルート・ハッシュ値を M(0,5) とする。このとき、タイプ２の監査情報内補完情報は、指定された識別番号が2 のとき、 [M(0,2)、M(0,3)、M(0,4)]となる。そして、監査装置5は上記の監査情報内補完情報を受信していれば、たとえTSA10が監査情報受信後に破綻したとしても、受理証明書が正しいことを検証することができる（例えば、クライアント装置3iが受け取った第1次二分木のルート・ハッシュ値M(0,2)と、監査情報に含まれたM(0,2)が一致すれば、クライアント装置3iの受理証明書の正しいことが検証できる）。

【０１３４】

また、本実施の形態の監査情報は、時刻証明装置１から監査装置５に自動的に送信される方式であったが、これとは異なり、監査装置５の方から監査情報の送信を時刻証明装置１に要求し、監査情報を受信することができるようにしてもよい。そして、いずれの方式においても、監査装置５にどのタイプの監査情報内補完情報を送信するかは、当該の監視／監査機関とTSA10の事前の契約により定められるものである。また、監査装置５の方から監査情報の送信を時刻証明装置１に要求し、監査情報を受信する方式においては、契約とは別に、要求時のオプションにより、監査情報内補完情報のタイプを指定できるようにしてもよい。

【０１３５】

尚、上記で説明した受理証明書に含まれる補完情報のパターン、及び監査情報に含まれる補完情報のパターンは、それぞれ組み合わせが可能であるが、例えば、受理証明書に含まれる補完情報のタイプ０、監査情報に含まれる補完情報のタイプ２の組み合わせの場合には、第２の検証を行うに際して、オンライン補完証明書は不要となるものである。これは、監査装置5がタイプ２の監査情報（監視点以前の第２次二分木のリーフ値すべて、即ち、第１次二分木のルート値すべて）を備えているので、この中にクライアント装置3iが受信した受理証明書に含まれる第１次二分木のルート値と同一のものがあるか否か検証

をすればよいからである。

【０１３６】

次に、監視点の決定方法について説明する。

【０１３７】

第２次二分木のどのリーフ（どの単位時間間隔）を監視点とするかは、例えば、以下の３つの方式が考えられるもので、どの方式も本実施の形態に適用可能なものである。

【０１３８】

方式１： 全ての単位時間間隔を監視点とする。

【０１３９】

方式２： Ｍ と ｍ を予め定められた整数とし、０ ≦ ｍ ＜ Ｍ を満たすものとし、当該の単位時間間隔を表す時刻値を所定の方法で整数に変換し、その結果を ｘ とする。

【０１４０】

ｘ ｍｏｄ Ｍ ＝ ｍ の時、当該の単位時間間隔を監視点とする。

【０１４１】

ここで、Ｍ が大きくなれば、監視される単位時間間隔の割合が減少し、それに応じて安全度も減少し、また監視のためのコストも減少する。Ｍ の決め方は、求められる安全度と監視のためのコストを勘案して決める必要がある。

【０１４２】

方式３：上記と同様に Ｍ と ｍ を定める。この単位時間間隔に構成される第１次二分木のルートのラベル値を ｖ とすると、所定の方法で ｖ を整数 ｗ に変換する。

【０１４３】

ｗ ｍｏｄ Ｍ ＝ ｍ の時、当該の単位時間間隔を監視点とする。

【０１４４】

次に、監査装置５の選定方法について説明する。

【０１４５】

本実施の形態においては、受理証明書に対応する監査情報を送信した監査装置５に対して、クライアント装置3iは監査要求を行うことを前提として説明し、監査装置５の選定については特に記載しなかった。以下においては、監視／監査機関が複数ある場合に特定の監査機関を選定するアルゴリズムについて説明するが、該アルゴリズムは、ある監視点において監査情報が送信される監査装置５を前もって予想することが困難であるようなものが望ましく、例えば、以下の方式が考えられる。

【０１４６】

方式１：

(1) 監査機関の全体の個数を Ｎ とし、各監査機関には ０ から Ｎ-1 までの番号を割り当てる。

【０１４７】

(2) 第１次二分木のルート値を所定の方法で整数に変換し、その値を ｘ とし、
ｘ ｍｏｄ Ｎ を計算して ｉ とおき、ｉ を番号とするような監査機関を選ぶ。

【０１４８】

そして、このようにして選ばれた監査機関の監査装置５に監査情報を送信する。

【０１４９】

また、１つの監視点において監査情報が送信される監査装置5は複数であってもよいとすると、例えば以下の方式が考えられる。

【０１５０】

方式２：

(1) 上記と同じく、監査機関の全体の個数を Ｎ とし、各監査機関には ０ から Ｎ-1 までの番号を割り当てる。

【０１５１】

(2) 1≦ Ｎ’ ＜ Ｎ となるような Ｎ’ を選ぶ。

【０１５２】

(3) 第１次二分木のルート値を所定の方法で整数に変換し、その値を ｘ とし、ｘ mod N' を計算して ｉ とおき、ｎ mod N' = ｉとなるような番号 ｎ を割り当てられた複数の監査機関を選ぶ。

【０１５３】

そして、このようにして選ばれた監査機関の監査装置５に監査情報を送信する。

【０１５４】

尚、上述の監査機関選定のアルゴリズムは、クライアント装置3iにも組み込まれているもので、これにより、クライアント装置3iは、時刻証明装置１と同様に第１次二分木のルート値から、監査を依頼すべき監査装置５を特定できるようになっている。

【０１５５】

尚、第１の実施の形態においては、ＴＳＡ10が、公開期間を定め、各公開期間におおける第２次二分木を構成し、そのルートに割り付けられた値を、公開メディア等に公開することを前提としていたが、この方法以外に、監査機関が、既に終了した公開期間に発行された受理証明書に対応することも含めて、長期に渡って受理証明書の保証書の発行を続けることにより、第２次二分木のルートの値を公開メディア等などに公表することを前提としない方式としてもよい。

【０１５６】

＜第２の実施の形態＞

図10は、本発明の第２の実施の形態に係るタイムスタンプ・システム200のシステム構成図である。同図に示すタイムスタンプ・システム200は、ＴＳＡ10に設けられた時刻証明装置1、ＴＡ20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置203ｉ（ｉは自然数）、監視／監査機関に設けられ、時刻証明装置1が発行した受理証明書に関する監査情報を公表する監査装置6、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置203ｉからのタイムスタンプ要求（時刻証明要求）に応えて、タイムスタンプつき受理証明書をクライアント装置203ｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置203ｉは、時刻証明装置1がメディア等40に公表した情報、又は、監査装置5から公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

【０１５７】

尚、上記コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【０１５８】

即ち、タイムスタンプ・システム100においては、監査装置5はクライアント装置３ｉの検証要求を受け付けて自ら検証を行っていたが、タイムスタンプ・システム200においては、監査装置6は監査情報を公開するだけであり、クライアント装置203ｉが自ら検証を行うようになっており、この点が両タイムスタンプ・システムの相違点となっている。尚、本実施の形態においては、第１の実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０１５９】

監査装置6は、コンピュータネットワーク4を介して時刻証明装置1およびクライアント装置203ｉとデータを送受信する送受信51、時刻証明装置1から送信された監査情報を記憶する監査情報記憶部52、およびこの監査情報をWeb上に公開する監査情報公開部63を具備している。

【０１６０】

クライアント装置203ｉは、コンピュータネットワーク4を介して時刻証明装置1および監査装置6とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置1からの時刻証明要求に対する受理証明書TSC(H

, t）を記憶する受理証明書記憶部34、および受理証明書TSC(H, t)を検証する時刻証明検証部36を具備している。尚、時刻証明検証部36は、定期的にメディア等40に公表される公表情報を利用して検証を行う第１の検証機能と、メディア等公表前に監査装置6を利用して検証を行う第２の検証機能とを備えるものである。

【０１６１】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（ＣＰＵ：Central Processing Unit）、プログラムやデータを収納する機能を有するＲＡＭ(Random Access Memory) 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、監査装置6の監査情報公開部63、およびクライアント装置203ｉの時刻証明検証部36の処理は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。

【０１６２】

次に、以上の構成を有するタイムスタンプ・システム200における時刻証明検証方法を図11を用いて説明する。ここで、図11は、時刻証明装置1が第２次二分木のルート値RHをメディア等40に公表する前に、クライアント装置203ｉが受理証明書TSC(H,t) の検証を行う動作（クライアント装置203ｉの第２の検証機能に相当する）を説明するシーケンス図である。尚、タイムスタンプ・システム200における時刻証明方法、監査装置5が監査情報の検証を行う動作、およびメディア等公表後にクライアント装置203ｉが受理証明書TSC(H,t)の検証を行う動作（クライアント装置203ｉの第１の検証機能に相当する）は、第１の実施の形態と同様であるため、説明を省略する。

【０１６３】

但し、ここで検証を行うクライアント装置203iを使用する利用者30は、検証の対象となる受理証明書TSC(H,t)を要求し取得した時刻証明要求者、及びこの時刻証明要求者から受理証明書TSC(H,t)を渡された時刻証明検証者の双方が考えられる。

【０１６４】

まず、クライアント装置203ｉが、検証する時点における後付２次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップＳ61）。この要求を時刻証明装置1が送受信部11を介して受信すると、時刻証明作成部14は、後付２次補完情報の一部（この時点において取得できる後付２次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置203ｉに送信する（ステップＳ62, Ｓ63, Ｓ64）。

【０１６５】

これにより、クライアント装置203ｉは、オンライン補完証明書を取得するので、時刻証明検証部36は、これに既に受け取っている１次情報および即時２次補完情報を加えて、当該の受理証明書に対応する第２次二分木のリーフから該第２次二分木のルートに向かうパスに属するノードのラベル値のうち計算可能なものを計算する（ステップＳ65, Ｓ66, Ｓ67）。

【０１６６】

次に、時刻証明検証部36は、監査装置6から公開されている監査情報の中から自己の受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査情報が存在するか否かを確認する（ステップＳ68, Ｓ69）。尚、監査情報は、図７に示す監査情報の時刻検証において監査情報に付された時刻が正しい場合（ステップＳ303）に、公開されるものである。

【０１６７】

このような監査情報 AI(H', t') が Web上に存在する場合には、該監査情報（該監査情報による、当該の受理証明書に対する認証点のラベル値、及び監査情報に付された時刻値を含むもの）を取得し、そこに含まれる認証点のラベル値Ａと，上記計算（ステップＳ65, Ｓ66, Ｓ67）により求めた認証点のラベル値Ａcal とが一致するか否かを検証し、この検証に成功した場合には、受理証明書TSC(H,t)に付された時刻の真正性についても検証する

（ステップＳ70，Ｓ71，S72，Ｓ73）。これは監査情報AI(H',t')に付された時刻から受理証明書TSC(H,t)に付されるべき時刻を算出し、該算出した時刻と受理証明書TSC(H,t)に付された時刻との差が一定時間内か否かを検証するものである。

【０１６８】

以上より、監査装置6に受理証明書TSC(H,t)の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査情報AI(H',t')が存在し、かつそれぞれの検証において、検証に成功すれば，受理証明書 TSC(H,t) が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップＳ74）。一方，いずれかの検証に失敗、もしくは監査装置６に受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査用情報が存在しない場合には、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップＳ75）。これにより，メディア等公表前においても，時刻証明装置1が発行した受理証明書TSC(H, t)を的確に検証でき，時刻情報やデータの真正性を明確にすることができる。

【０１６９】

以上、第２の実施の形態のタイムスタンプ・システム200によれば、第１の実施の形態のタイムスタンプ・システム100と同様の効果を得ることができる。加えて、本実施の形態においては、メディア等40に公表する前であっても，クライアント装置203ｉ自らで受理証明書TSC(H,t)の検証をすることができる。

【０１７０】

尚、第２の実施の形態のタイムスタンプ・システム200は、上述した形態に限定されるものではなく、第１の実施の形態のタイムスタンプ・システム100に施すことが可能であった種々のバリエーションをタイムスタンプ・システム200に適用することが可能なものである。

【０１７１】

＜第３の実施の形態＞

図12は、本発明の第３の実施の形態に係るタイムスタンプ・システム300のシステム構成図である。同図に示すタイムスタンプ・システム300は、ＴＳＡ10に設けられた時刻証明装置7、利用者30が利用する複数のクライアント装置303ｉ（ｉは自然数）、監視／監査機関に設けられ、時刻証明装置7が発行した受理証明書に関する監査情報を公表する監査装置8、時刻タグを供給する時刻タグシステム800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置7がクライアント装置303ｉからのタイムスタンプ要求（時刻証明要求）に応えて、タイムスタンプつき受理証明書をクライアント装置303ｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置303ｉは、時刻証明装置7がメディア等40に公表した情報、又は、監査装置8から公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

【０１７２】

また、タイムスタンプ・システム300は、時刻のトレーサビリティを確保する役割を時刻タグシステム800に集約しているので、ＴＳＡ 10は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置7が付与する時刻が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグτとは、所定の方法と手段により生成される乱数（但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する）であり、時刻タグシステム800を介して、各時刻タグに対応する時刻値を取得することができるものである。また、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０１７３】

時刻タグシステム800は、時刻タグ作成業者801が作成した時刻タグτをデジタル放送業者に802に提供すると、デジタル放送業者802は、この時刻タグτを時刻タグ認証業者803および時刻証明装置7に供給するようになっている。また、時刻タグ認証業者803は、受け取った時刻タグτと時刻源である時刻情報提供装置2から提供される時刻値を対応付けて管理しているので、監査装置8から時刻タグτと時刻値との対応に関する問い合わせがあった場合には、監査装置8に時刻タグτに対応する時刻値を回答できるようになっている。

【０１７４】

時刻証明装置7は、コンピュータネットワーク4を介して監査装置8、クライアント装置303ｉ、および時刻タグシステム800とデータを送受信する送受信部11、受理証明書に使用する時刻タグτを時刻タグシステム800から取得する時刻タグ情報取得部73、複数のクライアント装置303ｉからの時刻証明要求として送信されたメッセージ・ダイジェスト（デジタル・データから作成されるハッシュ値）および時刻タグ情報取得部73で取得した時刻タグτを二分木を用いてまとめる時刻証明要求まとめ部72、受理証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部72でまとめられたメッセージ・ダイジェストに対して時刻情報取得部13で取得した時刻情報を付して受理証明書を作成する時刻証明作成部14、定期的にメディア等40にデータを公表する時刻証明公表部15、時刻証明作成部14で作成された受理証明書を記憶する受理証明書記憶部16、および監査装置8に送信する監査情報（監査用受理証明書））を作成する監査情報作成部77を具備している。

【０１７５】

尚、ここで、時刻証明要求まとめ部72は、クライアント装置303iから送信されたメッセージ・ダイジェストに加えて時刻タグシステム800から取得した時刻タグτを第１次二分木のリーフに割り当てる点が時刻証明要求まとめ部12と異なっている。即ち、時刻タグτは、第１次二分木の所定のリーフ（予め定められた方法に従って、少なくとも１箇所以上）に、メッセージ・ダイジェストの代わりに割り付けられ、メッセージダイジェストと同様に扱われるものである。これにより、第１次二分木のリーフは、メッセージダイジェスト又は時刻タグが割り当てられる。

【０１７６】

また、監査情報作成部77は、作成する監査情報（監査用受理証明書）の構成において、監査情報作成部17と異なっているものである。より詳しくは、本実施の形態における受理証明書 TSC(H,t) は、第１次二分木のルート値H、該ルート値Hの識別番号、それぞれのラウンドに付与される時刻ｔ、１次補完情報HK1、および２次補完情報HK2を含む構成となっており、また、監査用受理証明書 TSC'(H',t') は、第１次二分木のルート値H、該ルート値Hの識別番号、１つの時刻タグτ（監査点において複数の時刻タグが割り当てられる場合には、任意の１つ）、それぞれのラウンドに付与される時刻ｔ、１次補完情報HK1、および２次補完情報HK2を含む構成となっている。

【０１７７】

図4に受理証明書TSC(H, t)の構成を示す。尚、図4に示す受理証明書TSC(H,t)は、上述したようにクライアント装置303iから送信されたメッセージ・ダイジェストそのものを第１次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第１次二分木のリーフに割り付けてもよく、この場合には、図5に示すように受理証明書TSC(H, t)は、キー付ハッシュ関数を適用する際のハッシュ・キーκも含む必要がある。より詳しくは、メッセージ・ダイジェストyを含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キーκを決定し、κをキーとして、yに対して、所定のキー付ハッシュ関数 h'を作用させ、ハッシュ値 h'(κ,y) を計算し、該ハッシュ値h'(κ,y)を第１次二分木のリーフに割り当てるものでこれにより、あるクライアント装置303iの送信したメッセージ・ダイジェストを他のクライアント装置303iに知られないようにすることが可能となる。

【０１７８】

図13に監査用受理証明書 TSC'(H',t')の構成を示す。図13に示すように監査用受理証明書 TSC'(H',t')は、受理証明書TSC(H, t)と同様に構成されるが、受理証明書においては当該のクライアント装置303iから送信されたメッセージ・ダイジェストを置くフィールドに、時刻タグτを置く点が受理証明書とは異なる点である。尚、図13は第１次二分木のリーフに割り付ける値として、クライアント装置303iから送られたメッセージ・ダイジェストあるいは取得した時刻タグをそのまま用いた場合の監査用受理証明書TSC'(H',t')の構成示すものであるが、受理証明書TSC(H,t)の場合と同様に、第１次二分木のリーフに、クライアント装置303 iから送られたメッセージ・ダイジェストあるいは時刻タグのキー付ハッシュ値を割り付けることも可能であり、この場合の監査用受理証明書TSC'(H',t')の構成は、図14に示す通りである。

【０１７９】

尚、時刻証明装置7から受理証明書TSC(H, t)をクライアント装置303iへ送信する際には，受理証明書TSC(H, t) の完全性の保証を高める補助手段として，時刻証明装置7が準備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけて送信するようにしてもよい。この場合，当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置303iからアクセス可能になっているものとする。

【０１８０】

監査装置8は、コンピュータネットワーク4を介して時刻証明装置7、クライアント装置303ｉ、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7から送信された監査情報（監査用受理証明書 TSC'(H',t')）を記憶する監査情報記憶部82、および監査情報（監査用受理証明書 TSC'(H',t')）の検証を行い、その結果をWeb上に公表する時刻証明公表部83を具備している。

【０１８１】

クライアント装置303ｉは、コンピュータネットワーク4を介して時刻証明装置7、監査装置8および時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7からの時刻証明要求に対する受理証明書 TSC(H,t) を記憶する受理証明書記憶部34、および受理証明書 TSC(H,t) を検証する時刻証明検証部37を具備している。尚、時刻証明検証部37は、定期的にメディア等40に公表される公表情報を利用して検証を行う第１の検証機能と、メディア等公表前に監査装置8を利用して検証を行う第２の検証機能とを備えるものである。

【０１８２】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（ＣＰＵ：Central Processing Unit）、プログラムやデータを収納する機能を有するＲＡＭ(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置7の時刻証明要求まとめ部72、時刻タグ情報取得部73、および監査情報作成部77、監査装置8の時刻証明公表部83、並びにクライアント装置303ｉの時刻証明検証部37の処理は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、監査装置8の監査情報記憶部82は、上記主記憶装置の機能を備えたものである。

【０１８３】

次に、以上の構成を有するタイムスタンプ・システム300における時刻証明方法、および時刻証明検証方法を図15乃至図18を用いて説明する。ここで、図15は、一公表サイクルにおいて時刻証明装置7が受理証明書TSC(H,t)を作成する動作を説明するシーケンス図であり、図16は、監査装置8が監査用受理証明書TSC'(H',t')の時刻付与に不正がないことを検証する動作を説明するフローチャートであり、図17及び図18は、時刻証明装置7が第２次二分木のルート値RHをメディア等40に公表する前に、クライアント装置303iが受理証明書 TSC(H,t)の検証を行う動作（クライアント装置303ｉの第２の検証機能に相当する）を説明するシーケンス図である。尚、メディア等公表後にクライアント装置303ｉが受理証

明書 TSC(H,t)の検証を行う動作（クライアント装置303iの第１の検証機能に相当する）は、第１および第２の実施の形態と同様であるため、説明を省略する。

【０１８４】

まず、時刻証明方法について説明する。クライアント装置303ｉが時刻証明装置7にメッセージ・ダイジェストyを含む時刻証明要求を送信すると、時刻証明装置7は送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部72が、このメッセージ・ダイジェストyを第１次二分木のリーフに割り当てる（ステップＳ201，Ｓ202，Ｓ203）。また、時刻証明要求まとめ部72aは、処理中の単位時間において時刻タグ放送業者から受信した時刻タグのうちから、前もって定められた選別手順に従って全部または一部を選び出し，当該の単位時間に対応する第1次二分木のリーフのなかから前もって定められた手順に従って選ばれた一部のリーフに割り当てる（ステップＳ203）。そして、同一ラウンド内においては、複数のクライアント装置303ｉから受信した複数の時刻証明要求に対して、第１次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部72がそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第１次二分木のルート値Hを計算する（ステップＳ204，Ｓ205）。

【０１８５】

次に、時刻証明要求まとめ部72が、第１次二分木のルート値Hを第２次二分木のリーフに割り当てて、インクリメンタルに第２次二分木を構成していくとともに、時刻証明作成部14は、クライアント装置303iから送信されたメッセージ・ダイジェストy、第１次二分木のルート値H、該ルート値Hの識別番号 n、時刻ｔ、１次補完情報HK1、および２次補完情報HK2 を含む受理証明書 TSC(H,t) を作成し、送受信部11を介してクライアント装置303ｉに受理証明書 TSC(H,t) を送信する（ステップＳ206，Ｓ207，Ｓ208）。

【０１８６】

これにより、クライアント装置303ｉは、受理証明書 TSC(H,t) を取得することができる（ステップＳ209）。尚、受理証明書 TSC(H,t) に含まれる２次補完情報には、この時点において取得できる即時２次補完情報は含まれているが、後付２次補完情報は含まれていない。

【０１８７】

次に、第１次二分木のルート値Hが割り当てられた第２次二分木のリーフが、監視点である場合には、監査情報作成部77が、監査情報（監査用受理証明書 TSC'(H'，t')）を作成し、該監査情報（監査用受理証明書 TSC'(H',t')）を送受信部11を介して監査装置8に送信する（ステップＳ210，Ｓ211，Ｓ212）。これにより、監査装置8は、監査情報（監査用受理証明書 TSC'(H',t')）を取得することができる（ステップＳ213）。

【０１８８】

そして、一定期間内においては、上述した時刻証明装置7の動作は繰り返され、一定期間が終了すると、時刻証明作成部74は、送受信部11を介して、クライアント装置303ｉに後付２次補完情報を含む補完証明書を送信する（ステップＳ214，Ｓ215）。これにより、クライアント装置303ｉは、受理証明書 TSC(H,t) とその全ての２次補完情報を取得したことになる（ステップＳ216）。また、時刻証明公表部15は、第２次二分木のルート値RHを計算し、このルート値RHをメディア等40に公表する（ステップＳ217，Ｓ218）。

【０１８９】

次に、監査装置8の検証動作について説明する。監査装置8が、送受信部81を介して監査用受理証明書TSC'(H',t') を受信すると、時刻証明公表部83は、この監査用受理証明書TSC'(H',t') を受信したときの時刻 t1を取得する（ステップＳ81，Ｓ82）。尚、この時刻t1は、監視装置8が参照する時計から取得するものであるが、この時計はある一定程度の正確性が保たれているものである。

【０１９０】

次に、時刻証明公表部83は、監査用受理証明書 TSC'(H'，t') から時刻 t' を抽出し、この時刻 t' と時刻 t1 の時間差が一定時間ｄ１（例えば、1秒）以内であるか否かを検

証する（ステップＳ83, Ｓ84）。

【０１９１】

上記検証において時刻 t' と時刻 t1 の時間差が一定時間以内の場合には、続いて、時刻証明公表部83は、受信した監査用受理証明書 TSC'(H', t')に含まれる時刻タグ τ に対応する時刻 t''を時刻タグ認証業者803から取得し（ステップＳ85）、この時刻 t''と時刻 t'の時間差が一定時間ｄ２（例えば、1秒）以内であるか否かを検証する（ステップＳ85, Ｓ86）。

【０１９２】

以上の検証それぞれにおいて、時間差が一定時間以内であれば、受信した監査用受理証明書 TSC'(H', t')の時刻は正しいということが証明される（ステップＳ87）。一方、いずれかの検証において時間差が一定時間以内でなければ、監査用受理証明書 TSC'(H',t') の時刻は不正であることが証明される（ステップＳ88）。これにより、本来、直近に受信した時刻タグ τ を用いて監査用受理証明書 TSC'(H',t') を発行する時刻証明装置7が、何らかの不正動作により、古い時刻タグ τ を用いて監査用受理証明書 TSC'(H', t') を発行するということを確実に排除することができる。そして、時刻証明公表部83は、検証の結果、監査用受理証明書 TSC'(H', t') の時刻が正しいと判断した場合には、Web上に監査用受理証明書 TSC'(H', t') を公開する（ステップＳ89）。

【０１９３】

次に、監査装置8を用いた時刻証明検証方法について説明する。まず、クライアント装置303ｉの時刻証明検証部37は、時刻証明装置7に送信した時刻証明要求に含まれるメッセージ・ダイジェスト、受信した受理証明書 TSC(H,t) に含まれる１次補完情報から第１次二分木のルート値 Hcal を計算する（ステップＳ311）。次に、時刻証明検証部37は、計算したルート値Hcal と受理証明書 TSC(H,t) に含まれる第１次二分木のルート値Hとが一致するか否かを検証する（ステップＳ312）。

【０１９４】

そして、ステップＳ312において、第１次二分木のルート値が一致した場合には、 検証する時点における後付２次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップＳ313）。この要求を時刻証明装置7が送受信部11を介して受信すると、時刻証明作成部14は、後付２次補完情報の一部（この時点において取得できる後付２次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置303ｉに送信する（ステップＳ314, Ｓ315, Ｓ316）。

【０１９５】

これにより、クライアント装置303ｉは、オンライン補完証明書を取得するので、時刻証明検証部37は、これに既に受け取っている受理証明書TSC(H,t)（１次情報および即時２次補完情報、並びに受理証明書TSC(H,t)に付された時刻）を加えて、当該の受理証明書に対応する第２次二分木のリーフから該第２次二分木のルートに向かうパスに属するノードのラベル値のうち計算可能なものを計算する（ステップＳ317, Ｓ318, Ｓ319）。

【０１９６】

次に、時刻証明検証部37は、監査装置8にアクセスし、Web上に公開している情報の中に自己の受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査用受理証明書TSC'(H',t')が存在するか否かを確認する（ステップＳ320, Ｓ321）。このような監査用受理証明書TSC'(H',t')がWeb上に存在する場合には、該監査用受理証明書（該監査用受理証明書による、当該の受理証明書に対する認証点のラベル値、及び監査用受理証明書に付された時刻値を含むもの）を取得して、そこに含まれる認証点のラベル値Ａと、上記計算（ステップＳ317, Ｓ318, Ｓ319）により求めた認証点のラベル値Ａcal とが一致するか否かを検証し、この検証に成功した場合には、さらに、受理証明書TSC(H,t)に付された時刻の真正性についても検証する（ステップＳ322, Ｓ323, Ｓ324, Ｓ325）。これは監査用受理証明書TSC'(H',t')に付された時刻から受理証明書TSC(H,t)に付されるべき時刻を算出し、該算出した時刻と受理証明書TSC(H,t)に付された時刻との差が一

定時間内か否かを検証するものである。

【０１９７】

以上より、監査装置8に受理証明書TSC(H,t)の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査用受理証明書TSC'(H',t')が存在し、かつ、それぞれの検証において、検証に成功すれば、受理証明書 TSC(H,t) が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップＳ326）。一方，いずれかの検証に失敗、もしくは監査装置8に受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第１次二分木のルート値の識別番号と等しいか、あるいは大きい第１次二分木のルート値の識別番号を含むような）監査用受理証明書が存在しない場合には、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップＳ327）。これにより、メディア等公表前においても、時刻証明装置7が発行した受理証明書 TSC(H, t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【０１９８】

以上、第３の実施の形態のタイムスタンプ・システム300によれば、第１の実施の形態のタイムスタンプ・システム100と同様の効果を得ることができる。加えて、本実施の形態のタイムスタンプ・システム300においては、時刻タグシステム800を備えることにより、時刻証明装置7が付与する時刻値が本来の時刻より過去になることを確実に防止する効果を備えている。

【０１９９】

尚、第３の実施の形態のタイムスタンプ・システム300は、上述した形態に限定されるものではなく、時刻タグの取得方法、受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、監査機関の選択方法、補完証明書の種類などについて種々のバリエーションを施すことが可能である。以下、このことについて説明する（受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、及び補完証明書の種類については、第１の実施の形態のタイムスタンプ・システム100で説明した内容と同一であるため、省略する）。

【０２００】

まず、時刻タグの取得方法について説明する。

【０２０１】

本実施の形態においては、 時刻証明装置７が、時刻タグシステム800から時刻タグτを取得して、第１次二分木の一部のリーフに時刻タグτ割り当てる方式について説明したが、これとは異なり、監査装置８が時刻タグシステム800から時刻タグτを取得して、該時刻タグτを時刻証明装置７に送信し、時刻証明装置７が第１次二分木の一部のリーフに受信した時刻タグτを割り当てる方式にしてもよい。

【０２０２】

この方式の場合に監査装置８が受信する監査用受理証明書の構成は、上述した図13及び図14と同じでもよいが、図19及び図20に示すような構成を採用してもよい。この場合においては、監査装置８が時刻タグシステム800から受信した時刻タグτのキー付ハッシュ値を時刻証明装置７に送信し、時刻タグτのキー付ハッシュ値を第１次二分木のリーフに割り当てる値とする。尚、図19は、クライアント装置303iから送信された時刻証明要求に含まれるメッセージ・ダイジェストを第１次二分木のリーフに割り当てる場合、図20は、クライアント装置303iから送信された時刻証明要求に含まれるメッセージ・ダイジェストのキー付ハッシュ値を第１次二分木のリーフに割り当てる場合を示している。

【０２０３】

次に、監査装置８の選定方法について説明する。

【０２０４】

本実施の形態においては、受理証明書に対応する監査情報を送信した監査装置８に対し

て、クライアント装置303iは監査要求を行うことを前提として説明し、監査装置８の選定については特に記載しなかった。以下においては、監視／監査機関が複数ある場合に特定の監査機関を選定するアルゴリズムについて説明するが、該アルゴリズムは、ある監視点において監査情報が送信される監査装置８を前もって予想することが困難であるようなものが望ましく、例えば、以下の方式が考えられる。

【０２０５】

方式１：

(1) 監査機関の全体の個数を N とし、各監査機関には 0 から N-1 までの番号を割り当てる。

【０２０６】

(2) 本実施の形態の時刻証明方法においては、その第１次二分木のリーフには一般に複数の時刻タグ $\tau(1), \cdots, \tau(k)$ が割り当てられている。

【０２０７】

そして、各々の時刻タグ $\tau(i)$ $(i = 1, \cdots, k)$ に応じて、異なる監査用受理証明書TSC(1), …, TSC(k)が生成される。

【０２０８】

(3) 各 $i = 1, \cdots, k$ に対して、以下の手順を実行する。

【０２０９】

(3-1) 時刻タグ $\tau(i)$ を所定の方法で整数に変換し、その値を $x(i)$ とし、$x(i) \bmod N$ を計算して $j(i)$ と置く。

【０２１０】

(3-2) $j(i)$ を番号とするような監査機関を $TSC(i)$ の送付先として選択する。

【０２１１】

そして、このようにして選ばれた監査機関の監査装置8に監査情報を送信する。

【０２１２】

また、１つの監視点において監査情報が送信される監査装置8は複数であってもよいとすると、例えば以下の方式が考えられる。

【０２１３】

方式２：

(1) 上記と同じく、監査機関の全体の個数を N とし、各監査機関には 0 から N-1 までの番号を割り当てる。

【０２１４】

(2) $1 \leq N' < N$ となるような N' を選ぶ。

【０２１５】

(3) 本実施の形態の時刻証明方法においては、その第１次二分木のリーフには一般に複数の時刻タグ $\tau(1), \cdots, \tau(k)$ が割り当てられている。

【０２１６】

そして、各々の時刻タグ $\tau(i)$ $(i = 1, \cdots, k)$ に応じて、異なる監査用受理証明書TSC(1), …, TSC(k)が生成される。各 $i = 1, \cdots, k$ に対して，以下の手順を実行する。

【０２１７】

(3-1) 時刻タグ $\tau(i)$ を所定の方法で整数に変換し、その値を $x(i)$ とし、$x(i) \bmod N'$ を計算して $j(i)$ と置く。

【０２１８】

(3-2) $n \bmod N' = j(i)$ となるような番号 n を割り当てられ監査機関を $TSC(i)$ の送付先として選択する。

【０２１９】

そして、このようにして選ばれた監査機関の監査装置8に監査情報を送信する。

【０２２０】

尚、本実施の形態においては、時刻証明装置７は、クライアント装置303iからの時刻証明要求を第１次二分木に集約し、該第１次二分木に対して時刻を割り付けていた。しかし

、このような第１次二分木を用いての集約を行わず、各時刻証明要求に対して時刻を割り付け、受理証明書を発行し、同時に上述した方法に従って、該受理証明書の監査を行う監査機関を決定し、ＴＳＡ10と複数の監査機関が連動する時刻証明システムを構成するようにしてもよい。これにより、ＴＳＡ10 を完全には信頼しなくても、システム全体の信頼性を確保することができる。さらに、第１次二分木を用いての集約は行うが、第２次二分木を用いての集約は行わない方法も考えられるが、これに関しては第３の実施の形態の変形例として後述する。

【０２２１】

また、本実施の形態においては、公開期間を定め、各公開期間で第２次二分木を構成し、そのルートに割り付けられた値を、公開メディア等に公開することを前提としていた。この方法以外に、監査機関が、既に終了した公開期間に発行された受理証明書に対応することも含めて、長期に渡ってWeb等への掲載を続けることにより、第２次二分木のルートの値を公開メディア等などに公表することを前提としない方式としてもよい。

【０２２２】

さらに、本実施の形態においては、受理証明書TSC(H,t)に時刻タグτを含めていなかったが、受理証明書TSC(H,t)に時刻タグτを付加するようにしてもよい。これにより、上述の監査機関選定のアルゴリズムをクライアント装置303iに組み込めば、クライアント装置303iは、監査を依頼すべき監査装置8をクライアント装置303i自身で選定することができるというメリットがある。尚、受理証明書に時刻タグτを含めた場合の受理証明書の構成を、図21及び図22に示す。

【０２２３】

＜第３の実施の形態の変形例＞

図37は、本発明の第３の実施の形態の変形例であるタイムスタンプ・システム310のシステム構成図である。同図に示すタイムスタンプ・システム310は、ＴＳＡ10に設けられた時刻証明装置7a、利用者30が利用する複数のクライアント装置303ａｉ（ｉは自然数），監視／監査機関に設けられ、時刻証明装置7aが発行した受理証明書に関する監査情報を公表する監査装置8a、時刻タグを供給する時刻タグシステム800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置7aがクライアント装置303ａｉからのタイムスタンプ要求（時刻証明要求）に応えて、タイムスタンプつき受理証明書をクライアント装置303ａｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置303ａｉは、監査装置8aから公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

【０２２４】

また、タイムスタンプ・システム310は、時刻のトレーサビリティを確保する役割を時刻タグシステム800に集約しているので、ＴＳＡ 10は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置7aが付与する時刻が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグτとは、所定の方法と手段により生成される乱数（但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する）であり、時刻タグシステム800を介して、各時刻タグに対応する時刻値を取得することができるものである。また、本変形例においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０２２５】

時刻証明装置7aは、コンピュータネットワーク4を介して監査装置8a、クライアント装置303ａｉ、および時刻タグシステム800とデータを送受信する送受信部11、受理証明書に使用する時刻タグτを時刻タグシステム800から取得する時刻タグ情報取得部73、複数のクライアント装置303ａｉからの時刻証明要求として送信されたメッセージ・ダイジェスト（デジタル・データから作成されるハッシュ値）および時刻タグ情報取得部73で取得した時刻タグτを二分木を用いてまとめる時刻証明要求まとめ部72ａ、受理証明書を作成する

際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部72aでまとめられたメッセージ・ダイジェストに対して時刻情報取得部13で取得した時刻情報を付して受理証明書 TSC(H,t) を作成する時刻証明作成部14a、時刻証明作成部14aで作成された受理証明書TSC(H,t)を記憶する受理証明書記憶部16、および監査装置8aに送信する監査情報（監査用受理証明書TSC'(H,t)）を作成する監査情報作成部77aを具備している。

【０２２６】

尚、ここで、時刻証明要求まとめ部72a は、クライアント装置303aiから送信されたメッセージ・ダイジェストに加えて時刻タグシステム800から取得した時刻タグτを第１次二分木のリーフに割り当てる点、及び第２次二分木を作成しない点（但し、第１次二分木のルート値に対する識別番号の取得は行う）が、時刻証明要求まとめ部12と異なっている。即ち、時刻タグτは、第１次二分木の所定のリーフ（予め定められた方法に従って、少なくとも１箇所以上）に、メッセージ・ダイジェストの代わりに割り付けられ、メッセージダイジェストと同様に扱われるものである。これにより、第１次二分木のリーフは、メッセージダイジェスト又は時刻タグが割り当てられる。

【０２２７】

また、時刻証明作成部14a、及び監査情報作成部77aは、それぞれ作成する受理証明書、及び監査情報（監査用受理証明書）の構成において、時刻証明作成部14、及び監査情報作成部17と異なっているものである。より詳しくは、本実施の形態における受理証明書 TSC(H,t) は、第１次二分木のルート値H、該ルート値Hの識別番号、それぞれのラウンドに付与される時刻ｔ、および１次補完情報HK1を含む構成となっており、また、監査用受理証明書 TSC'(H',t') は、第１次二分木のルート値H、該ルート値Hの識別番号、１つの時刻タグτ（監査点において複数の時刻タグが割り当てられる場合には、任意の１つ）、それぞれのラウンドに付与される時刻ｔ、および１次補完情報HK1を含む構成となっている。

【０２２８】

図38に受理証明書TSC(H, t)の構成を示す。尚、図38に示す受理証明書TSC(H,t)は、上述したようにクライアント装置303aiから送信されたメッセージ・ダイジェストそのものを第１次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第１次二分木のリーフに割り付けてもよく、この場合には、図39に示すように受理証明書TSC(H, t)は、キー付ハッシュ関数を適用する際のハッシュ・キーκも含む必要がある。より詳しくは、メッセージ・ダイジェストyを含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キーκを決定し、κをキーとして、yに対して、所定のキー付ハッシュ関数 h'を作用させ、ハッシュ値 h'(κ,y)を計算し、該ハッシュ値h'(κ,y)を第１次二分木のリーフに割り当てるものでこれにより、あるクライアント装置303aiの送信したメッセージ・ダイジェストを他のクライアント装置303aiに知られないようにすることが可能となる。

【０２２９】

図40に監査用受理証明書 TSC'(H,t)の構成を示す。図40に示すように監査用受理証明書 TSC'(H', t')は、受理証明書TSC(H, t)と同様に構成されるが、受理証明書においては当該のクライアント装置303aiから送信されたメッセージ・ダイジェストを置くフィールドに、時刻タグτを置く点が受理証明書とは異なる点である。尚、図40は第１次二分木のリーフに割り付ける値として、クライアント装置303aiから送られたメッセージ・ダイジェストあるいは取得した時刻タグをそのまま用いた場合の監査用受理証明書TSC'(H, t'の構成示すものであるが、受理証明書TSC(H,t)の場合と同様に、第１次二分木のリーフに、クライアント装置303a iから送られたメッセージ・ダイジェストあるいは時刻タグのキー付ハッシュ値を割り付けることも可能であり、この場合の監査用受理証明書TSC'(H,t)の構成は、図41に示す通りである。

【０２３０】

尚、時刻証明装置7aから受理証明書TSC(H,t)をクライアント装置303aiへ送信する際には，受理証明書TSC(H, t) の完全性の保証を高める補助手段として，時刻証明装置7aが準

備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけて送信するようにしてもよい。この場合，当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置303aiからアクセス可能になっているものとする。

【０２３１】

監査装置8ａは、コンピュータネットワーク4を介して時刻証明装置7a、クライアント装置303ａｉ、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7aから送信された監査情報（監査用受理証明書 TSC'(H,t)）を記憶する監査情報記憶部82、および監査情報（監査用受理証明書 TSC'(H,t)）の検証を行い、その結果をWeb上に公表する時刻証明公表部83aを具備している。

【０２３２】

クライアント装置303ａｉは、コンピュータネットワーク4を介して時刻証明装置7a、監査装置8aおよび時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7aからの時刻証明要求に対する受理証明書 TSC(H,t) を記憶する受理証明書記憶部34、および受理証明書 TSC(H, t) を検証する時刻証明検証部37aを具備している。尚、時刻証明検証部37aは、監査装置8を利用して検証を行う検証機能を備えるものである。

【０２３３】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（ＣＰＵ：Central Processing Unit）、プログラムやデータを収納する機能を有するＲＡＭ(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置7aの時刻証明要求まとめ部72a、時刻証明作成部14a、および監査情報作成部77a、監査装置8aの時刻証明公表部83a、並びにクライアント装置303ａｉの時刻証明検証部37aの処理は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。

【０２３４】

次に、以上の構成を有するタイムスタンプ・システム310における時刻証明方法、および時刻証明検証方法を図42乃至 図45を用いて説明する。ここで、図42は、時刻証明装置7aが受理証明書TSC(H,t)を作成する動作を説明するシーケンス図であり、図43は、クライアント装置303aiが受理証明書 TSC(H,t)の検証を行う動作を説明するシーケンス図である。尚、監査装置8aが監査用受理証明書 TSC'(H,t)の時刻付与に不正がないことを検証する動作については、第３の実施の形態と同様であるため、説明を省略する。

【０２３５】

まず、時刻証明方法について説明する。クライアント装置303ａｉが時刻証明装置7aにメッセージ・ダイジェストyを含む時刻証明要求を送信すると、時刻証明装置7aは送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部72aが、このメッセージ・ダイジェストyを第１次二分木のリーフに割り当てる（ステップＳ401，Ｓ402，Ｓ403）。また時刻証明要求まとめ部72aは、処理中の単位時間において時刻タグ放送業者から受信した時刻タグのうちから、前以って定められた選別手順に従って全部または一部を選び出し，当該の単位時間に対応する1次二分木のリーフのなかから前以って定められた手順に従って選ばれた一部のリーフに割り当てる。そして、同一ラウンド内においては、複数のクライアント装置303ａｉから受信した複数の時刻証明要求に対して、第１次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部72aがそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第１次二分木のルート値Hを計算する（ステップＳ404，Ｓ405）。

【０２３６】

時刻証明作成部14aは、第１次二分木のルート値Hの識別番号を割り当て、クライアント装置303iから送信されたメッセージ・ダイジェストy、第１次二分木のルート値H、該ルート値Hの識別番号 n、時刻ｔ、１次補完情報HK1を含む受理証明書 TSC(H,t) を作成し、

送受信部11を介してクライアント装置303aiに受理証明書 TSC(H,t) を送信する（ステップS406, S407, S408）。これにより，クライアント装置303aiは、受理証明書 TSC(H,t) を取得することができる（ステップS409）。

【0237】

次に、監査情報作成部77aが、監査情報（監査用受理証明書 TSC'(H,t)）を作成し、該監査情報（監査用受理証明書 TSC'(H, t)）を送受信部11を介して監査装置8aに送信する（ステップS410, S411）。これにより，監査装置8aは、監査情報（監査用受理証明書 TSC'(H',t')）を取得することができる（ステップS412）。

【0238】

次に、監査装置8aを用いた時刻証明検証方法について説明する。まず、クライアント装置303aiの時刻証明検証部37aは、時刻証明装置7aに送信した時刻証明要求に含まれるメッセージ・ダイジェスト、受信した受理証明書 TSC(H,t) に含まれる1次補完情報から第1次二分木のルート値 Hcal を計算する（ステップS431）。次に、時刻証明検証部37aは、計算したルート値Hcal と受理証明書 TSC(H,t) に含まれる第1次二分木のルート値Hとが一致するか否かを検証する（ステップS432）。

【0239】

そして、ステップS432において、第1次二分木のルート値が一致した場合には、 時刻証明検証部37は、監査装置8aにアクセスし、Web上に公開している情報の中に自己の受理証明書に対応する監査用受理証明書TSC'(H,t)が存在するか否かを確認する（ステップS433, S434）。監査用受理証明書TSC'(H,t)がWeb上に存在する場合には、受理証明書TSC(H, t) に含まれる第1次二分木のルート値と監査用受理証明書TSC'(H,t)に含まれるの第1次二分木のルート値が一致するか否か検証する（ステップS435, S436）。

【0240】

以上より、監査装置8aに受理証明書TSC(H,t)に対応する監査用受理証明書TSC'(H,t)が存在し、かつ、検証に成功すれば、受理証明書 TSC(H,t) が改ざんされていないことに加えて，当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップS437）。一方、検証に失敗、もしくは監査装置8aに受理証明書TSC(H,t)に対応する監査用受理証明書TSC'(H,t)が存在しない場合には、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップS438）。これにより、時刻証明装置7aが発行した受理証明書 TSC(H, t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【0241】

以上、第3の実施の形態の変形であるタイムスタンプ・システム310によれば、第1の実施の形態のタイムスタンプ・システム100と同様に TSAを完全に信頼しなくとも監査機関を用いることにより，受理証明書の真正性検証することができる。 加えて、タイムスタンプ・システム310においては、時刻タグシステム800を備えることにより、時刻証明装置7が付与する時刻値が本来の時刻より過去になることを確実に防止する効果を備えている。

【0242】

尚、タイムスタンプ・システム310においては、受理証明書TSC(H,t)に時刻タグτを含めていなかったが、受理証明書TSC(H,t)に時刻タグτを付加するようにしてもよい。これにより、上述の監査機関選定のアルゴリズムをクライアント装置303aiに組み込めば、クライアント装置303aiは、監査を依頼すべき監査装置8aをクライアント装置303i自身で選定することができるというメリットがある。尚、受理証明書に時刻タグτを含めた場合の受理証明書の構成を、図44及び図45に示す。

【0243】

＜第4の実施の形態＞

図23は、本発明の第4の実施の形態に係るタイムスタンプ・システム400のシステム構成図である。同図に示すタイムスタンプ・システム400は、ＴＳＡ10に設けられた時刻証

明装置7、利用者30が利用する複数のクライアント装置403ｉ（ｉは自然数）、監視／監査機関に設けられ、時刻証明装置7が発行した受理証明書の保証書を作成する監査装置9、時刻タグを供給する時刻タグシステム800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置7がクライアント装置403ｉからのタイムスタンプ要求（時刻証明要求）に応えて、タイムスタンプつき受理証明書をクライアント装置403ｉに返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置403ｉは、時刻証明装置7がメディア等40に公表した情報、又は、監査装置9から送信された受理証明書の保証書によって受理証明書を検証できるようになっているコンピュータシステムである。

【０２４４】

尚、上記コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【０２４５】

また、第３の実施の形態と同様に、タイムスタンプ・システム400は、時刻のトレーサビリティを確保する役割を時刻タグシステム800に集約しているので、ＴＳＡ10は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置7が付与する時刻値が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグτとは、所定の方法と手段により生成される乱数（但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する）であり、時刻タグシステム800を介して、各時刻タグに対応する時刻値を取得することが出来るものである。また、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０２４６】

監査装置9は、コンピュータネットワーク4を介して時刻証明装置7、クライアント装置403ｉ、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7から送信された監査情報（監査用受理証明書 TSC'(H',t')）の検証を行い、その結果として監査用受理証明書TSC'(H',t')の保証書を作成するとともに、クライアント装置403からの時刻証明要求を監査用受理証明書TSC'(H',t')の保証書を用いて検証する時刻証明検証部93、および監査用受理証明書TSC(H,t)、及び監査用受理証明書TSC'(H',t')の保証書を記憶する監査情報記憶部92、を具備している。

【０２４７】

クライアント装置403ｉは、コンピュータネットワーク4を介して時刻証明装置7、監査装置9および時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7からの時刻証明要求に対する受理証明書TSC(H,t)を記憶する受理証明書記憶部34、および受理証明書TSC(H,t)を検証する時刻証明検証部38を具備している。尚、時刻証明検証部38は、定期的にメディア等40に公表された公表情報を利用して検証を行う第１の検証機能と、メディア等公表前に監査装置9を利用して検証を行う第２の検証機能とを備えるものである。

【０２４８】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（ＣＰＵ：Central Processing Unit）、プログラムやデータを収納する機能を有するＲＡＭ(Random Access Memory) 等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、監査装置9の時刻証明検証部93、およびクライアント装置403ｉの時刻証明検証部38の処理は、上記ＣＰＵによる演算制御機能を具体的に示したものに他ならない。また、監査装置9の監査情報記憶部92は、上記主記憶装置の機能を備えたものである。

【０２４９】

次に、以上の構成を有するタイムスタンプ・システム400における時刻証明検証方法を

図24乃至図26を用いて説明する。ここで、図24は、監査装置9が監査用受理証明書TSC'(H',t')の時刻付与に不正がないことを検証する動作を説明するフローチャートであり、図25及び図26は、時刻証明装置7が２次二分木のルート値RHをメディア等40に公表する前に、クライアント装置403ｉが受理証明書TSC(H,t)の検証を行う動作（クライアント装置403ｉの第２の検証機能に相当する）を説明するシーケンス図である。尚、タイムスタンプ・システム400における時刻証明方法、およびメディア等公表後にクライアント装置303ｉが受理証明書TSC(H,t)の検証を行う動作（クライアント装置403ｉの第１の検証機能に相当する）は、第３の実施の形態と同様であるため、説明を省略する。

【０２５０】

まず、監査装置9の検証動作について説明する。監査装置9が、送受信部81を介して監査用受理証明書TSC'(H',t')を受信すると、時刻証明検証部93は、この監査用受理証明書TSC'(H',t')を受信したときの時刻 t1を取得する（ステップＳ101、Ｓ102）。尚、この時刻t1は、監視装置9が参照する時計から取得するものであるが、この時計はある一定程度の正確性が保たれているものである。

【０２５１】

次に、時刻証明検証部93は、監査用受理証明書 TSC'(H',t') から時刻t'を抽出し、この時刻 t' と時刻 t1 の時間差が一定時間ｄ１（例えば、1秒）以内であるか否かを検証する（ステップＳ103, Ｓ104）。

【０２５２】

上記検証において時刻 t' と時刻 t1 の時間差が一定時間以内の場合には、続いて、時刻証明検証部93は、受信した監査用受理証明書 TSC'(H',t')に含まれる時刻タグτに対応する時刻 t''を時刻タグ認証業者803から取得し（ステップＳ105）、この時刻 t''と時刻 t'の時間差が一定時間ｄ２（例えば、1秒）以内であるか否かを検証する（ステップＳ105, Ｓ106）。

【０２５３】

以上の検証それぞれにおいて、時間差が一定時間以内であれば、受信した監査用受理証明書 TSC'(H',t')の時刻は正しいということが証明される（ステップＳ107）。一方、いずれかの検証において時間差が一定時間以内でなければ、監査用受理証明書 TSC'(H',t')の時刻は不正であることが証明される（ステップＳ108）。これにより、本来、直近に受信した時刻タグτを用いて監査用受理証明書 TSC'(H',t') を発行する時刻証明装置7が、何らかの不正動作により、古い時刻タグτを用いて監査用受理証明書TSC'(H', t') を発行するということを確実に排除することができる。そして、時刻証明検証部93は、検証の結果、監査用受理証明書 TSC'(H',t') の時刻が正しいと判断した場合には、デジタル署名を付した監査用受理証明書TSC'(H',t')の保証書を作成し、監査情報記憶部92に記憶させる（ステップＳ109）。尚、このデジタル署名は、「この監査用受理証明書の時刻タグ付けは正しい」ということを意味するメッセージＲＭのハッシュ値に対して署名鍵 SK を用いてデジタル署名をしたものであり、監査用受理証明書の保証書は、該デジタル署名sig(SK,h(RM))、メッセージＲＭ、および監査用受理証明書TSC'(H',t') を含む構成となっている。

【０２５４】

次に、監査装置9を用いた時刻証明検証方法について説明する。まず、クライアント装置403ｉの時刻証明検証部38は、時刻証明装置7に送信した時刻証明要求であるメッセージ・ダイジェスト、受信した受理証明書TSC(H,t)に含まれる１次補完情報から第１次二分木のルート値Hcal を計算する（ステップＳ111）。次に、時刻証明検証部38は、計算したルート値Hcal と受理証明書TSC(H,t)に含まれる第１次二分木のルート値Hとが一致するか否かを検証する（ステップＳ112）。

【０２５５】

そして、ステップＳ112において、第１次二分木のルート値が一致した場合には、 検証する時点における後付２次補完情報を含むオンライン補完証明書を時刻証明装置7に要求する（ステップＳ113）。この要求を時刻証明装置7が送受信部11を介して受信すると、

時刻証明作成部14は、後付２次補完情報の一部（この時点において取得できる後付２次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置403ｉに送信する（ステップＳ114, Ｓ115, Ｓ116）。

【０２５６】

これにより、クライアント装置403ｉは、オンライン補完証明書を取得するので、時刻証明検証部38は、これに既に受け取っている受理証明書TSC(H,t)（１次情報および即時２次補完情報、並びに受理証明書TSC(H,t)に付された時刻）を加えた検証要求情報を監査装置9に送信する（ステップＳ117, Ｓ118）。

【０２５７】

次に、監査装置9が検証要求情報を送受信部81を介して受信すると、時刻証明検証部93は、受理証明書に対応する監査用受理証明書の保証書が監査情報記憶部92に存在するか否かを確認して、保証書が存在する場合には、監査用受理証明書の保証書を取得する（ステップＳ119, Ｓ120, Ｓ121）。

【０２５８】

そして、保証書が存在する場合には、受信した検証要求情報から認証点のラベル値Ａcal を計算し、監査情報として既に受け取っているこの認証点のラベル値Ａを監査情報記憶部92から取得して、この認証点のラベル値Ａが、計算により求めた認証点のラベル値Ａcal に一致するか否かを検証する（ステップＳ122, Ｓ123）。そして、この検証に成功した場合には、受理証明書TSC(H,t)に付された時刻の真正性についても検証する（ステップＳ124, S125）。これは監査情報に付された時刻から受理証明書TSC(H,t)に付されるべき時刻を算出し、該算出した時刻と受理証明書に付された時刻との差が一定時間内か否かを検証するものである。

【０２５９】

以上より、監査装置9に受理証明書に対応する監査用受理証明書の保証書が存在し、かつ、それぞれの検証において、検証に成功すれば、受理証明書TSC(H,t)が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップＳ126）。一方、いずれかの検証に失敗、もしくは監査装置9に受理証明書に対応する監査用受理証明書の保証書が存在しない場合には、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップＳ127）。

【０２６０】

監査装置9は、上記の検証結果を踏まえて、受理証明書が正しいと判断した場合には、監査用受理証明書の保証書、正しくないと判断した場合には、検証結果をクライアント装置403ｉに送受信部81を介して送信する（ステップ128）。

【０２６１】

クライアント装置403ｉは、送受信部31を介して監査用受理証明書の保証書を受信すると、時刻証明検証部38が署名鍵SK に対応する公開鍵PK を取り出し、受理証明書の保証書に含まれているデジタル署名 sig(SK,h(RM))が、監査用受理証明書の保証書に含まれているメッセージＲＭを含むデジタル・データに対してなされたことを公開鍵PKを用い検証する（ステップＳ129, Ｓ130, Ｓ131）。

【０２６２】

以上、クライアント装置403ｉにおける検証において、検証に成功した場合には、受理証明書TSC(H,t) が正しいことを確認することができる（ステップＳ132）。一方、ステップＳ112、またはステップＳ131の検証に失敗した場合には、受理証明書TSC(H,t) が不正であることを確認することができる（ステップＳ133）。これにより、メディア等公表前においても、時刻証明装置7が発行した受理証明書TSC(H,t)を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【０２６３】

以上、第４の実施の形態のタイムスタンプ・システム400によれば、第３の実施の形態のタイムスタンプ・システムと同様の効果を得ることができる。加えて、本実施の形態の

タイムスタンプ・システム400においては、デジタル署名を用いた受理証明書の保証書を用いて受理証明書 TSC(H,t) の検証を行うので、データの守秘性をさらに高めることができる。

【０２６４】

尚、第４の実施の形態のタイムスタンプ・システム400は、上述した形態に限定されるものではなく、第３の実施の形態のタイムスタンプ・システム300に施すことが可能であった種々のバリエーションをタイムスタンプ・システム400に適用することが可能なものである（もちろん、第３の実施の形態の変形例であるタイムスタンプ・システム310に対応するタイムスタンプ・システム410を構築することも可能である）。

【０２６５】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対してさらに種々の変形や変更を施すことができる。例えば、上記実施の形態においては、時刻証明装置がメディア等40を利用して第２次二分木のルート値RHを定期的にメディア等40に公表してきたが、メディア等40を利用する代わりに、コンピュータネットワーク4で接続されている公表装置（オンラインサーバ）が、第２次二分木のルート値RHを保持し、クライアント装置にＦＴＰやＨＴＴＰなどのプロトコルを用いて提供するようにしてもよい。ここで、公表装置に関しては、メディア等40に公表する目的、即ち、多数の第三者に保証の拠り所となる値を公開し記録させることによって、その値の改竄を不可能にするという目的、と同一の目的を達成するためには、一定数以上の複数の公表装置が独立に運営されている必要がある。尚、前提として、公表装置は、時刻証明装置から第２次二分木のルート値RHが送信されるようになっている、もしくは、第２次二分木のリーフに割り当てる値から第２次二分木を構成するようになっているものである。また、クライアント装置における受理証明書の検証は、上記実施の形態と同様であるが、複数の公表装置を利用したそれぞれの検証結果が異なる場合には、一定数以上の公表装置をもとに同一検証結果が得られているかどうかにより、最終的な判定を下すものである。

【０２６６】

図27（ａ）は、上述した第２次二分木のルート値RHと一定期間との対応付けを掲載しているログファイル41の内容を示しているものである。このログファイル41は、一定期間毎に第２次二分木のルート値RHが順次追加されるとともに、公表装置を介して、クライアント装置に提供されるようになっている。

【０２６７】

尚、公表装置は、図27（ｂ）に示すように、ログファイル41のハッシュ値を計算し、該ハッシュ値を保持するとともに、該ハッシュ値を掲載しているファイル42をクライアント装置に提供するようにしてもよい。尚、この場合においては、クライアント装置からの要求に応じてログファイル41を別途を提供する必要があり、クライアント装置においては、ログファイル41から計算されるハッシュ値とファイル42に掲載されているハッシュ値が一致するか否かを検証することになる。そして、この場合においても、複数の公表装置を利用したそれぞれの検証結果が異なる場合には、一定数以上の公表装置をもとに同一検証結果が得られているかどうかにより、最終的な判定を下すことになる。

【０２６８】

従って、コンピュータネットワーク4に接続された公表装置を別途設ける方法によれば、時刻証明装置が保持すべき公表情報のコピーを公表装置がもつことになるので、当該データが事故などにより消失することを確実に防止することができる。さらに、ファイル42を公表情報とする方法においては、掲載情報は少なくて済むので、例えば、Webページの広告等に掲載することも可能であるとともに、公表装置に必要とされるストレージの量を大幅に減らすことができるという効果がある。

【０２６９】

尚、公表装置の機能を、監査装置に組み込んで、監査装置が定期的に受理証明書に関する情報を公表するようにしてもよい。この場合においては、監視装置を利用すれば、いか

なるときにおいても、利用者装置は受理証明書の検証をすることが可能となる。

【０２７０】

また、以上の上記実施の形態における各装置の動作は、各装置に格納されたプログラムを実行することにより実現される。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、コンピュータネットワークを介して配信することも可能である。

【０２７１】

＜第１次二分木の構成，および認証点の性質＞

上記実施の形態において用いられた第１次二分木の動的な構成方法、および認証点の性質について説明するが、その前提としてまず、二分木の構成に必要な基本関数について説明する。

【０２７２】

高さｋの二分木は、レベル0からレベルｋまでのノードで構成されるが、レベルｊ（ｊ＝0,1,…,k）のノードの数は、２（ｋ－ｊ）であるので、レベルｊ、番号ｉのノードを（ｊ，ｉ）と表すことにすると、ｉ＝0,1,…,2（k-j）-1となる。

【０２７３】

以下、実数ｘに対して、ceiling(x)をｘ以上の最小の整数、floor(x)をｘ以下の最大の整数として、説明する。

【０２７４】

ノード（ｊ，ｉ）（但し，ｊ＜ｋ）の親は、（ｊ＋1，floor(i/2))であるので、

patent（j,i）＝（ｊ＋1，floor(i/2)）と定義する。

【０２７５】

また、ノード（ｊ，ｉ）（但し，0＜ｊ）の左側の子供は（j-1，2i）、右側の子供は（j-1，2i+1）であるので、

leftChild（j,i）＝（j-1，2i）

rightChild（j,i）＝（j-1，2i+1）と定義する。

【０２７６】

このとき、高さｋの二分木のノードｊ，ｉ）（0≦ｉ＜2（k-j））のルートパス rtPath(k，j，ｉ)（ノード(j,i)からルートに至るノード(j,i)の列をいう)は、

rtPath(k,j,i)＝（（j,r(j)），…，（k,r(k)））と表せる。

【０２７７】

但し、r(j’)＝ｉ（j’＝j,…,k），r(j’+1)＝floor(r(j’)/2)（j’＜kとし、r(j’)は既に定まっているものとする）であるとする。尚、（k,r(k)）は、二分木のルートを表し、常にr(k)＝0となる。

【０２７８】

また、高さｋの二分木のノード（ｊ，ｉ）（0≦ｉ＜2（k-j））の認証パスauthPath(ノード(j,i)からルート値を計算するのに必要なノード(j,i)の集合。但し、該ノードを連接する方向（左又は右）の情報も含んでいる)は、rtPath(k,j,i) を用いて次のように表せる。

【０２７９】

authPath(k,j,i)＝（((j,a(j),LR(j))，…，((k-1,a(k-1),LR(k-1)))

ここで、r(j’)が偶数の場合、a(j’)＝r(j’)＋1，r(j’)が奇数の場合、r(j’)－1であり、また，r(j’)が偶数の場合、LR(j’)＝R，r(j’)が奇数の場合、LR(j’)＝Lである（但し，j’＝ j,…,k-1）。

【０２８０】

そして、authPath(k,j,i)の要素((j,a(j),LR(j))について、LR(j)の部分を（ＬＲ）タグという。さらに，rtPath(k,j,i)の要素（j,r(j))について、r(j)が偶数のとき、((j,r(j)+1),R) を(j,r(j))の右補完点という。r(j)が奇数のとき、((j,r(j)-1),L) を(j,r(j))を(j,r(j))の左補完点という。

【０２８１】
このとき、authPath(k,j,i)は、rtPath(k,j,i)のルート以外の点の右補完点あるいは左補完点からなる。
【０２８２】
上述した基本関数の定義のもと、第１の動的な第１次二分木の構成方法について説明する。この第１次二分木の構成方法は、深さの違いを1以内に押さえ、ダミーノードを作成しない方法である。
【０２８３】
単位時間（1ラウンドの時間であり，例えば，1秒）に受け付けた時刻証明要求の数をｎとすると、高さｋは，ｋ＝ceiling(log2(n))である。高さｋの二分木のリーフ数は最大で2kであるので、ｄ＝2k－ｎとして、レベル0のノードのうち、2ｄ個を消去すれば、時刻証明要求の数ｎをダミーノードなしでリーフに割り当てることが可能となる。これは、レベル0のリーフが2ｄ個減ると、レベル1のリーフが新たにｄ個できるので、合計でｄ個減り、リーフの数は結局，2k－ｄ＝ｎとなるからである。
【０２８４】
以下、L1W＝2（k-1）（レベル1のノードの個数）、L1L＝2（k-1）－ｄ（子を有するレベル1のノードの個数）の，L0L＝2（2（k-1）－ｄ）（レベル0のノードの個数）とおくと、ｎ個の時刻証明要求のうち、初めのL0L個をレベル0に配置し、残りをレベル1に配置するとき、ｉ番目の時刻証明要求の配置先を表す関数place(i)は次式で表すことができる。
【０２８５】
place(i)＝（0,i）　　（0≦i＜L0L）
place(i)＝（1，L1L + i - L0L）　　（L0L ＜ i ≦ n）
ここで、place(i)＝（レベル，番号）で構成されているものである。
【０２８６】
図28は、第１の動的な第１次二分木の構成方法のｎ＝10の場合の具体例を示すものである。この場合においては、図28に示す通り、ｋ＝ceiling(log2(10))＝4となり、高さは4である。そして，ｄ＝24－10＝6であるので、6×2＝12個のレベル0のリーフを消去する。この結果、L1W＝23＝8、L1L＝8－6＝2、L0L＝2×2＝4となる。従って、レベル0のリーフが4個、レベル1のリーフが6個で、リーフの合計数はｎ＝10となる。この結果，図28に示すような第１次二分木を動的に作成することができる。
【０２８７】
次に、第２の動的な第１次二分木の構成方法について説明する。この二分木の構成方法は、深さを単一にして，ダミーノードを作成する方法である。
【０２８８】
単位時間（1ラウンドの時間であり、例えば、1秒）に受け付けた時刻証明要求の数をｎとすると、高さｋは、ｋ＝ceiling(log2(n))である。高さｋの二分木のリーフ数は最大で2k であるので、0からｎ－1までのｎ個の時刻証明要求をレベル0のノード（0,0）からノード（0，n-1）に割り当てる。ここで、レベル0に割り当てられた、最も右のノード（0，n-1）に対して、ルートパス rtPath(k，0，n-1)を計算する。次に、各レベルｊ（ｊ＝0，…，k-1）においては、以下の手順を実行するものとする。
【０２８９】
r(j)が偶数のとき、ノード（j，r(j)+1）をダミーノードとする。
【０２９０】
r(j)+1＜ｉ＜2(k-j)となる各ｉに対して、ノード（ｊ，ｉ）は消去される。
【０２９１】
r(j)が奇数のとき、r(j)+1＜ｉ＜2(k-j)となる各ｉに対して、ノード（ｊ，ｉ）は消去される。また、ルートにあるレベルｋについては、何も行わない。
【０２９２】
以上のような方法に基づいて構成される二分木は、ダミーノードは各レベルの右端でのみ現れる、および作成されるダミーノードの数は、ｋ以下であるという性質を有する。

【０２９３】
図29は、第２の動的な第１次二分木の構成方法のｎ＝9の場合の具体例を示す図である。この場合においては、図29に示す通り，ｋ＝ceiling(log2(9))＝4となり、高さは4である。そして、9個の時刻証明要求をノード（0,0）…（0,n-1）に割り当てると、レベル0において時刻証明要求が割り当てられた最も右のノードは（0,8）である。
【０２９４】
ここで、ノード（0,8）のルートパス rtPath(4,0,8)は
rtPath(4,0,8)＝（(0,8)，(1,4)，(2,3)，(3,1)(4,0)）となる。これにより，各レベルでの手順は、以下の通りになる。
【０２９５】
レベル0では、（0,9）がダミーノードになり、番号10以降が消去される。レベル1では、（1,5）がダミーノードとなり、5＜ｉ＜23＝8であれば、ノード（ｊ，ｉ）は削除される。レベル2では、ノード（2,3）がダミーノードになる。レベル3および4においては、ダミーノードも消去されるノードもない。この結果，図29に示すような第１次二分木を動的に作成することができる。
【０２９６】
次に、第３の動的な二分木の構成方法について説明する。第１および第２の動的な第１次二分木の構成方法は、ともに受け付けた時刻証明要求の数が確定した後に、二分木を構成する方法であったが、この方法は、第２の動的な二分木の構成方法をベースに、インクリメンタルに第１次二分木を構成する方法である。ここで、イクリメンタルとは、時刻証明要求を受け付ける都度、そこから計算できる二分木の部分を計算していくという意味である。この意味で、前もって定めた時間間隔（ラウンドの時間）に受け付ける時刻証明要求の数は予想できないものとする。以下では、受け付ける時刻証明要求の数は予想できないが、その上界Ｎは見積もることができるとして説明する。尚、この方法においては、第２の動的な第１次二分木の構成方法と同様に、時刻証明要求はすべてレベル0に割り付けられるものとする（ダミーノードを使用する方法である）。
【０２９７】
図30は，第３の動的な第１次二分木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って第１次二分木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。
【０２９８】
・K＝ceiling(log2（N））とする。
【０２９９】
・nは受け付けた時刻証明要求の数を示す整数変数とする。初期値は0である。
【０３００】
・kは定められた時間間隔が終了したときの二分木の高さを表す変数とする。
【０３０１】
（K+1）個のカウンタの列を、i(0)，…，i(K)とする。ここで，i(j)の初期値は0である（j=0，…,K）。i(j)はレベルjにおいて、既に生成されたノードの数を表すと同時に、次にレベルjに作成されるノードの番号を表す。
【０３０２】
・（K+1）個のプール変数の列を、b(0)，…，b(K)とする。ここで，b(j)の初期値はfalseである（j=0，…,K）。b(j)は、レベルjにダミーノードがあるか否かを表す。
【０３０３】
・（K+1）個の配列の列を、A(0)，…，A(K)とする。各配列は、2(k-j)の長さをもち、レベルjのノードに割り付けられる値を保持する（j=0，…,K）。ノード(j,i)に対して、A(j,i)は，A(j)[i]を表すものとする。ノード(j,i)の左側の子が(j’，i’)のとき、A（leftChild(j,i)）はA(j’)[i’]を表す。
【０３０４】
・rはダミーノードに割り当てるダミー値を保存する変数である。

【０３０５】
・R(j,i)は2つの引数i,jに対してノード(j,i)に割り当てるべきダミー値を計算する関数である。
【０３０６】
・X，X0，X1，X2は，ノードに割り当てる値を表す変数である。
【０３０７】
・X1‖X2は、バイト列で表された2つの値の連接である。
【０３０８】
・h(x)はxのハッシュ値を計算する関数である。
【０３０９】
このような定義のもと，図30の処理手順1が終了すると（定められた時間が終了すると）、nは、受け付けた時刻処理要求の数、kは生成された二分木の高さ、i(j)は、レベルjのノードの数、b(j)は、レベルjにダミーノードがあるか否か、A（j）は、レベルjのノードに割り付けられた値、をそれぞれ有することになる。
【０３１０】
図31は、第３の動的な二分木の構成方法のｎ＝9の場合の具体例を示す図である。即ち、定められた時間間隔が終了したとき、ｎ＝9であったとする。このとき、ｋ＝ceiling(log2(9))＝4となり、高さは4の二分木を構成することになる。尚、0からｎ－1までのｎ個の時刻処理要求は、処理手順1により、既にノード(0,0)，…，(0,n-1)に割り当てられている。また、処理手順1により、i(0)＝9，i(1)＝4，i(3)＝1，i(4)＝0となっている。
【０３１１】
このとき、処理手順2の(2.2)から、ノード(0,9)のノートパスrtPath(4,0,9)は、rtPath(4,0,9)＝（(0,9)，(1,4)，(2,3)，(3,1)，(4,0)）となる。これから、各レベルの手順は、以下の通りになる。
【０３１２】
レベル0においては、ステップ（2.3.2.1）より、ノード（0,9）がダミーノードになる。レベル1においては、ステップ（2.3.2.1.5）より、ノード（1,4）に値が割り付けられ、(1,5)がダミーノードになる。レベル2においては、ステップ（2.3.2.1.5）より、ノード（0,2）に値が割り付けられ、(0,3)がダミーノードになる。レベル3においては、ステップ（2.3.2.1）により、ノード（3,1）に値が割り付けられる。レベル4においては、ステップ（2.3.2.1）により、ノード（4,0）に値が割り付けられる。
【０３１３】
この結果，図31に示すような第１次二部木をインクリメンタルに構成することができる。
【０３１４】
尚，上記実施の形態におけるタイムスタンプ・システム100、200、300および400は、上述した動的な第１次二分木の構成方法のいずれをも採用できるものであり、これにより、クライアント装置3ｉ、203ｉ、303ｉおよび403ｉからの時刻証明要求の量的変化に柔軟に対応することができるので，スケーラビリティの高いタイムスタンプ・システムを構築することが可能となる。
【０３１５】
次に、第２次二分木における対象点の監視点に対する認証点を計算するアルゴリズムについて、説明する。前提として、第２次二分木の高さをｋとし、対象点の番号をi0、監視点の番号をi1とし、i0＜i1とする。このとき、ノード（0，i0）のルートパス rtPath0 を計算する。同様に、ノード（0，i1）のルートパス rtPath1 を計算する。すると、rtPath0とrtPath1は、ある要素以降は一致する。このとき、最初に一致した要素を、ノード（0，i0）とノード（0，i0）の合流点（confluent point）と呼ぶ。そして、合流点のレフト・チャイルドを、ノード（0，i0）（対象点）のノード（0，i1）（監視点）に対する認証点（authentication point）とよぶ。
【０３１６】

一般に、i0＜i1のとき、認証点は以下の性質を有する。

【０３１７】

(1) 認証点のラベルは、監視点、即ち、ノード (0, i1) の受理証明書内補完情報 に含まれる。

【０３１８】

(2) ノード (0, i1) の時刻証明処理が終わった時点で、認証点のラベルは、対象点、即ち、ノード (0, i0) が受信できる受理証明書内補完情報およびオンライン補完証明書から計算することができる。

【０３１９】

以下、上記性質の証明を行う。ここで、合流点を (j, i) 、そのレフト・チャイルドである認証点を (j', i') とおく。まず、(1) について図32を用いつつ説明する。

【０３２０】

ノード (0, i1) のルートパス rtPath(k, 0, i1)において、(0, i1) から出発して、合流点に至る直前のノードを (j", i") とおく。このとき、認証点は, (j", i") の左補完点である。従って、認証パス authPath(k, 0, i1)の定義から、((j', i'), L)はノード (0, i1) の認証パスに含まれる。よって、((j', i'), L)は (0, i1) に対する受理証明書内補完情報に含まれる。

【０３２１】

次に (2) について図33および図34を用いつつ説明する。

【０３２２】

認証点 (j', i') はノード (0, i0) のルートパス rtPath(k, 0, i0)に含まれる。ここで、

rtPath(k, 0, i0) ＝((0,r(0)), …, (j' ,r(j')), (j' +1,r(j' +1)), …, (k,r(k))とする。

【０３２３】

j1 ＝ 0, …, j' に対して、ノード (j1, r(j1)) のラベルを、ノード (0, i1) の時刻証明処理が終わった時点で、ノード (0, i0) が受信できるオンライン補完証明書と受理証明書内補完情報、及びノード (0, i0) のラベルの情報から、以下のようにj1について再帰的に計算する。

【０３２４】

j1＝0のときは, r(0)＝i0だから、(j1, r(j1))＝ (0, i0) 。 (0, i0) のラベルを(j1, r(j1))のラベルとおく。

【０３２５】

次に、j2＜j1 (≦j') に対して、(j2, r(j2))のラベルは計算済みとする。これから(j1, r(j1))のラベルを以下のように計算する。

【０３２６】

rtPath(k, 0, i0)の高さ j1-1 の要素は、高さj1の要素の、レフト・チャイルドかライト・チャイルドである。どちらであるかによって場合分けする。

【０３２７】

(ａ) レフト・チャイルドであるとき、図33に示すように、rtPath(k, 0, i0)上の高さj1の点p3のラベルは、高さ j1-1 の点 p1 のラベルとその兄弟 p2 のラベルから合成される。高さ j1-1の点 p1 のラベルv1は計算済みである。一方p2のラベルv2は、(0, i1) の時刻証明処理が終わった時点で、(0,i0) が受信できるオンライン補完証明書に含まれる。なぜならば、(0,i1) の時刻証明処理が終わった時点で、図33のＡで表された部分木のラベルは計算可能であり、その時点でのオンライン補完証明書に含まれるからである。従って、(0,i0) の時刻証明要求者は、点p3のラベルv3は、次のように計算できる。

【０３２８】

v3＝h(v1 ‖ v2)

(ｂ) ライト・チャイルドであるとき、図34に示すように, rtPath(k, 0, i0)上の高さj1の点p3のラベルは、高さ j1 - 1 の点p1のラベルとその兄弟p2のラベルから合成される。

高さ j1 － 1 の点p1のラベルv1は計算済みである。一方点p2のラベルv2は、(0,i0)の要求者に対する受理証明書内補完情報に含まれる。従って、点p3のラベルv3は、次のように計算できる。

【０３２９】

$$v3 = h(v2 \| v1)$$

以上から、再帰法により、j1 ＝ 0, …,j' に対して、ノード(j1, r(j1))のラベルを、(0, i1)の処理が終わった時点で、(0, i0)の時刻証明要求者が受信できるオンライン補完証明書と(0, i0)の受理証明書内補完情報から計算することができる。従って，j1＝j'のラベル，即ち認証点のラベルも，(0, i0)の時刻証明要求者は計算することができる。

【図面の簡単な説明】

【０３３０】

【図１】本発明の第１の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図２】本発明の第１の実施の形態における第１次二分木の構成を説明する図である。

【図３】本発明の第１の実施の形態における第２次二分木の構成を説明する図である。

【図４】本発明の第１の実施の形態における受理証明書の構成を説明する図である。

【図５】本発明の第１の実施の形態における受理証明書の構成を説明する図である。

【図６】本発明の第１の実施の形態に係るタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。

【図７】本発明の第１の実施の形態に係るタイムスタンプ・システムの監査情報検証方法を説明するフローチャートである。

【図８】本発明の第１の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図９】本発明の第１の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図１０】本発明の第２の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図１１】本発明の第２の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図１２】本発明の第３の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図１３】本発明の第３の実施の形態における監査用受理証明書の構成を説明する図である。

【図１４】本発明の第３の実施の形態における監査用受理証明書の構成を説明する図である。

【図１５】本発明の第３の実施の形態に係るタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。

【図１６】本発明の第３の実施の形態に係るタイムスタンプ・システムの監査情報検証方法を説明するフローチャートである。

【図１７】本発明の第３の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。

【図１８】本発明の第３の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。

【図１９】本発明の第３の実施の形態における他の形式の監査用受理証明書の構成を説明する図である。

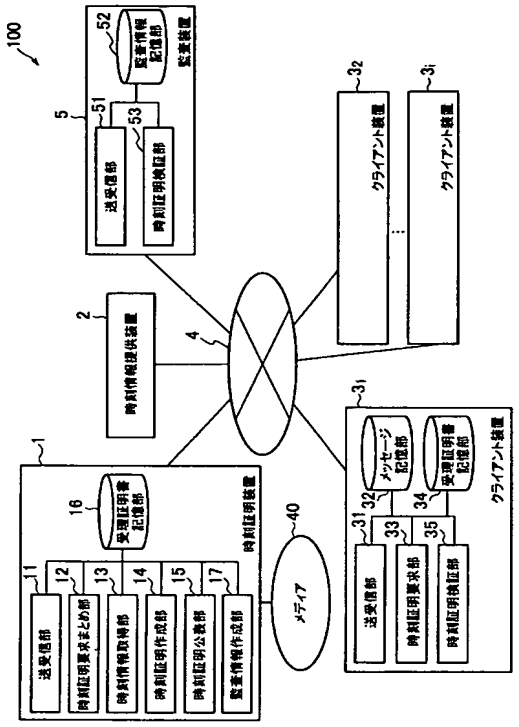
【図２０】本発明の第３の実施の形態における他の形式の監査用受理証明書の構成を説明する図である。

【図２１】本発明の第３の実施の形態における時刻タグを含む場合の受理証明書の構成を説明する図である。

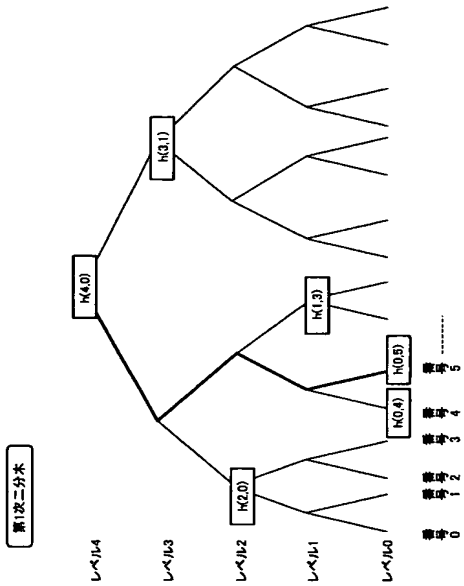
【図２２】本発明の第３の実施の形態における時刻タグを含む場合の受理証明書の構成を説明する図である。
【図２３】本発明の第４の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。
【図２４】本発明の第４の実施の形態に係るタイムスタンプ・システムの監査情報検証方法を説明するフローチャートである。
【図２５】本発明の第４の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。
【図２６】本発明の第４の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。
【図２７】公表装置が公表するファイルを説明する図である。
【図２８】深さの違いを1以内に押さえ、ダミーノードを作成しない動的な第１次二分木の構成方法を説明する図である。
【図２９】深さを単一にして、ダミーノードを作成する動的な第１次二分木の構成方法を説明する図である。
【図３０】インクリメンタルに第１次二分木を構成する方法のアルゴリズムを説明する図である。
【図３１】インクリメンタルに第１次二分木を構成する方法を説明する図である。
【図３２】第２次二分木における認証点を説明する図である。
【図３３】第２次二分木における認証点を説明する図である。
【図３４】第２次二分木における認証点を説明する図である。
【図３５】タイムスタンプ・システムの概念を説明する図である。
【図３６】線形リンキングを用いたタイムスタンプ・システムの概念を説明する図である。
【図３７】本発明の第３の実施の形態の変形例のタイムスタンプ・システムの構成を説明する図である。
【図３８】本発明の第３の実施の形態の変形例における受理証明書の構成を説明する図である。
【図３９】本発明の第３の実施の形態の変形例における受理証明書の構成を説明する図である。
【図４０】本発明の第３の実施の形態の変形例における監査用受理証明書の構成を説明する図である。
【図４１】本発明の第３の実施の形態の変形例における監査用受理証明書の構成を説明する図である。
【図４２】本発明の第３の実施の形態の変形例のタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。
【図４３】本発明の第３の実施の形態の変形例のタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。
【図４４】本発明の第３の実施の形態の変形例における時刻タグを含む場合の受理証明書の構成を説明する図である。
【図４５】本発明の第３の実施の形態の変形例における時刻タグを含む場合の受理証明書の構成を説明する図である。
【図４６】本発明の第１の実施の形態における受理証明書の他の構成を説明する図である。
【図４７】直前のラウンドの第１次二分木のルート値を現在の第１次二分木に割り当てる方法を説明する図である。
【図４８】直前のラウンドの第１次二分木のルート値を現在の第１次二分木に割り当てる方法を説明する図である。
【符号の説明】
【０３３１】

1,7,7a　時刻証明装置
2　時刻情報提供装置
3,203,303,303a,403　クライアント装置
4　コンピュータネットワーク
5,6,8,8a,9　監視装置
10　ＴＳＡ
11　送受信部
12,72,72a　時刻証明要求まとめ部
13　時刻情報取得部
14,14a　時刻証明作成部
15　時刻証明公表部
16　受理証明書記憶部
17,77,77a　監査情報作成部
20　ＴＡ
30　利用者
31　送受信部
32　メッセージ記憶部
33　時刻証明要求部
34　受理証明書記憶部
35,36,37,38　時刻証明検証部
40　メディア等
41,42　ファイル
51,81　送受信部
52,82,92　監査情報記憶部
53,93　時刻証明検証部
63　監査情報公開部
73　時刻タグ情報取得部
83,83a　時刻証明公表部
100,200,300,310,400,900,910　タイムスタンプ・システム
800　時刻タグシステム
801　時刻タグ作成業者
802　デジタル放送業者
803　時刻タグ認証業者

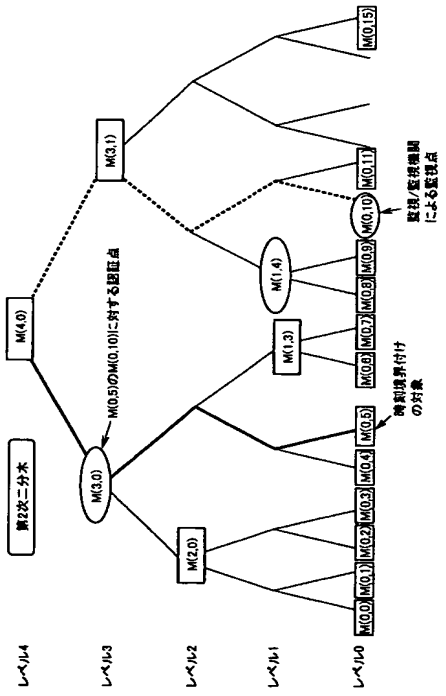
【図１】



【図２】



【図３】



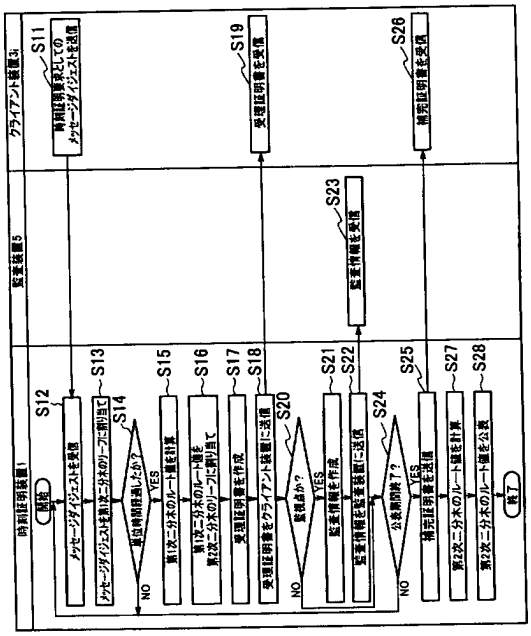
【図４】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	
2次補完情報	HK2	

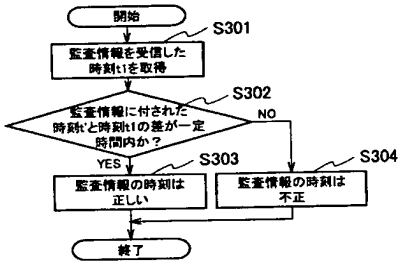
【図５】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付ハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	
2次補完情報	HK2	

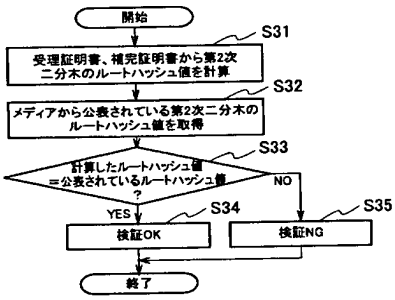
【図６】


クライアント装置3i
監査装置5
時刻証明装置1
開始
S11
時刻証明要求としてのメッセージダイジェストを送信
S19
受理証明書を受信
S26
補完証明書を受信
S23
監査情報を受信
S12
S13
S14
S15
S16
S17
S18
S20
S21
S22
S24
S25
S27
S28
メッセージダイジェストを受信
メッセージダイジェストを第1次二分木のリーフに割り当て
最終時刻経過したか？
YES
NO
第1次二分木のルート値を計算
第1次二分木のルート値を第2次二分木のリーフに割り当て
受理証明書を作成
受理証明書をクライアント装置に送信
監査値か？
YES
NO
監査情報を作成
監査情報を監査装置に送信
公表期限？？
YES
NO
補完証明書を送信
第2次二分木のルート値を計算
第2次二分木のルート値を公表
終了

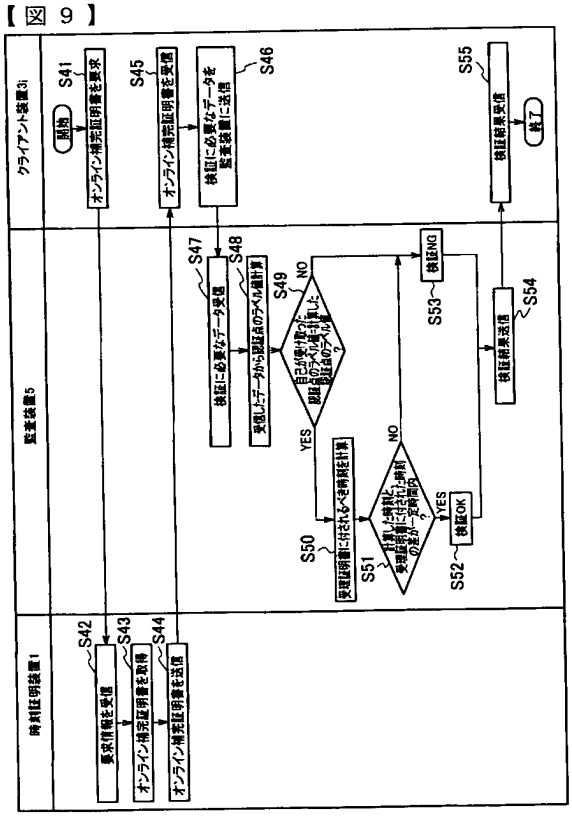
【図７】


開始
S301
監査情報を受信した時刻t1を取得
S302
監査情報に付された時刻t'と時刻t1の差が一定時間内か？
NO
YES
S303
監査情報の時刻は正しい
S304
監査情報の時刻は不正
終了

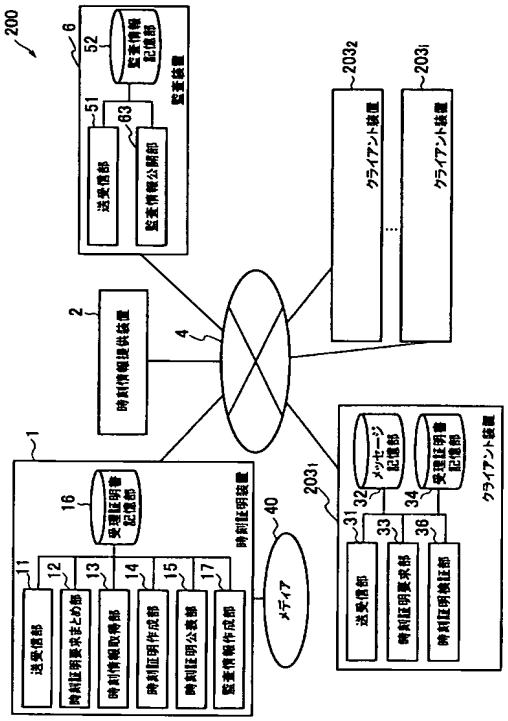
【図８】


開始
S31
受理証明書、補完証明書から第2次二分木のルートハッシュ値を計算
S32
メディアから公表されている第2次二分木のルートハッシュ値を取得
S33
計算したルートハッシュ値＝公表されているルートハッシュ値？
NO
YES
S34
検証OK
S35
検証NG
終了

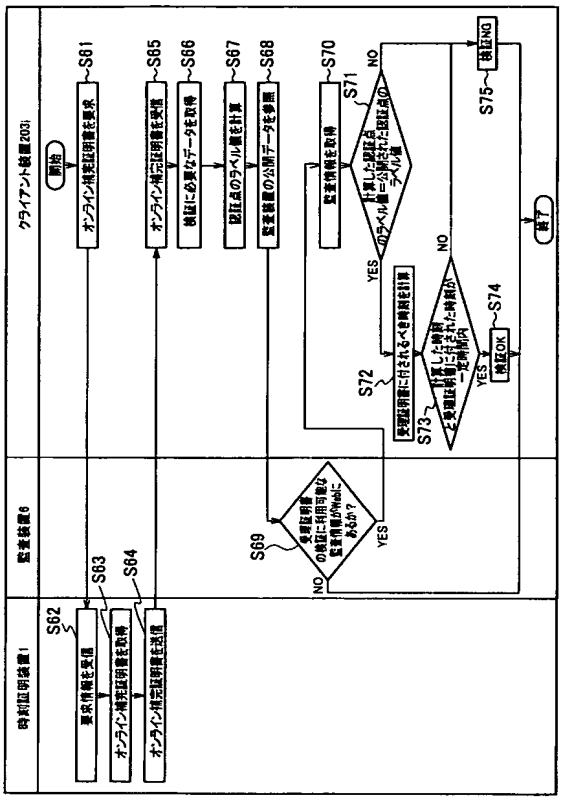
【図９】


クライアント装置3i
監査装置5
時刻証明装置1
開始
S41
オンライン補完証明書を要求
S45
オンライン補完証明書を受信
S46
検証に必要なデータを監査装置に送信
S55
検証結果受信
終了
S47
検証に必要なデータ受信
S48
受信したデータから認証点のラベル値計算
S49
NO
YES
S50
受理証明書に付されるべき時刻を計算
S51
S52
検証OK
S53
検証NG
S54
検証結果送信
S42
要求情報を受信
S43
オンライン補完証明書を取得
S44
オンライン補完証明書を送信

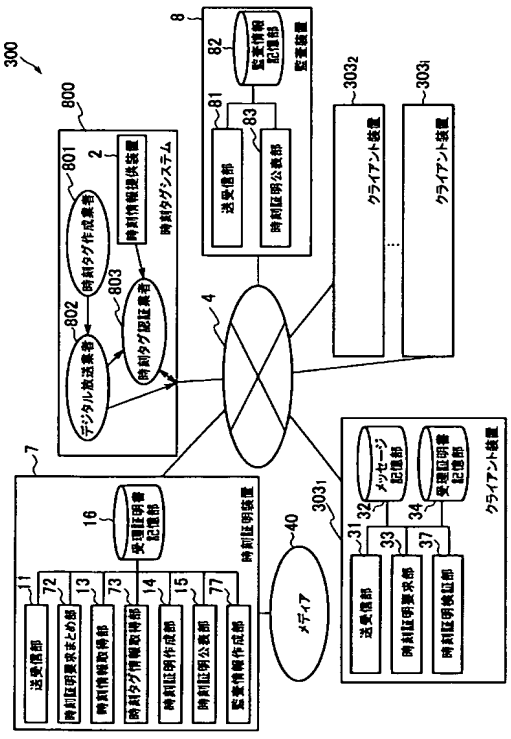
【図１０】



【図１１】



【図１２】



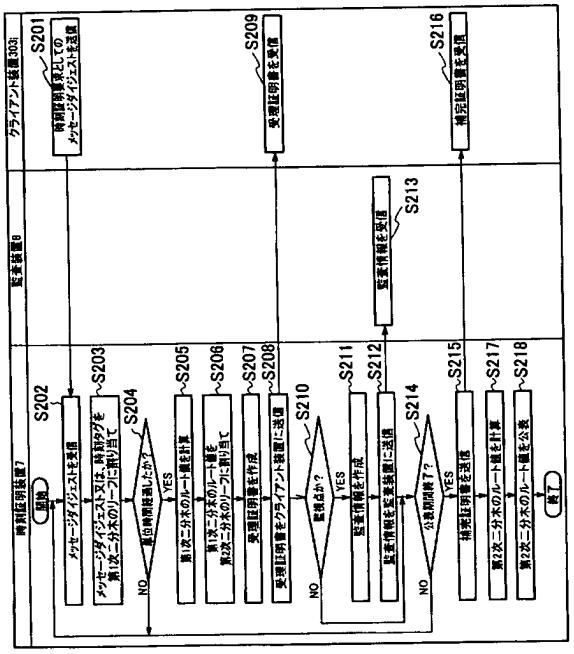
【図１３】

項目	記号	値の例
時刻タグ	τ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_H(0,4)),(R_H(1,3)),(L_H(2,0)),(R_H(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

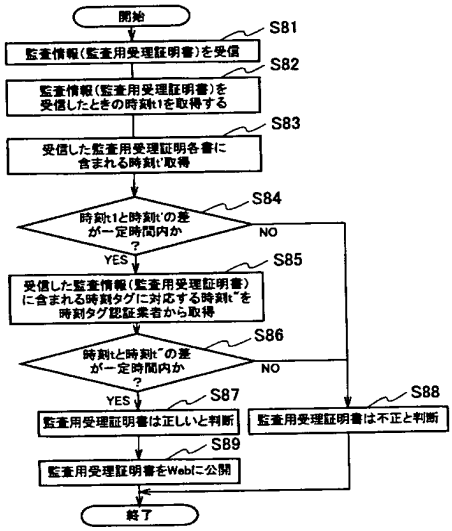
【図１４】

項目	記号	値の例
時刻タグ	τ	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	K	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_H(0,4)),(R_H(1,3)),(L_H(2,0)),(R_H(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

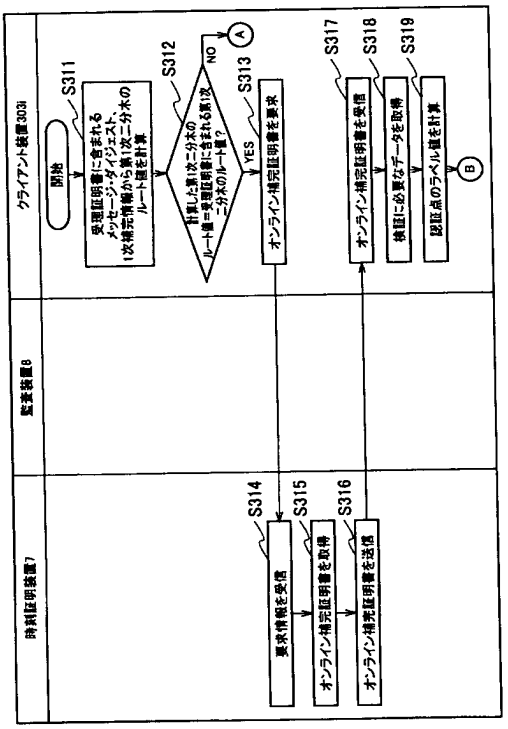
【図１５】



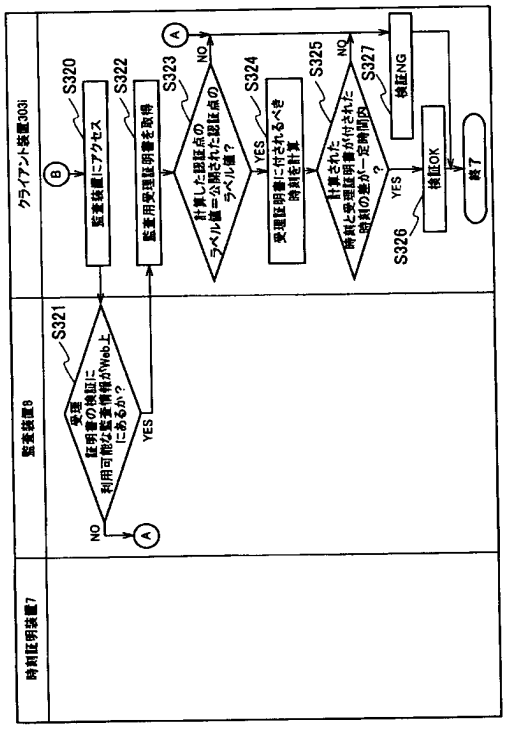
【図１６】



【図１７】



【図１８】



【図１９】

項目	記号	値の例
時刻タグのハッシュ値であるメッセージ・ダイジェスト	y	$y=h_\kappa(\kappa, r)$で、rは監査機関が受信した時刻タグ、h_κは所定のキー付ハッシュ関数、κはハッシュ・キー
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	
2次補完情報	HK2	

【図２０】

項目	記号	値の例
時刻タグのハッシュ値であるメッセージ・ダイジェスト	y	$y=h_\kappa(\kappa, r)$で、rは監査機関が受信した時刻タグ、h_κは所定のキー付ハッシュ関数、κはハッシュ・キー
時刻	t	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	κ	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	
2次補完情報	HK2	

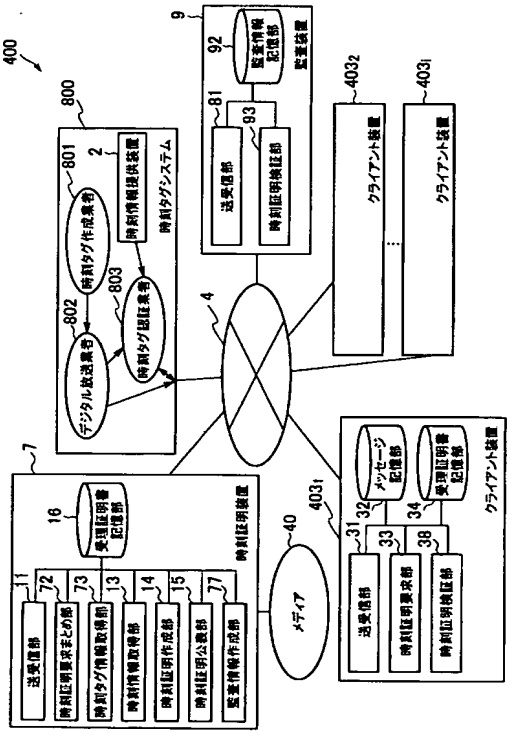
【図２１】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(r_1, \cdots, r_n)$	
第1次二分木のルート値	H	
2次補完情報	HK2	

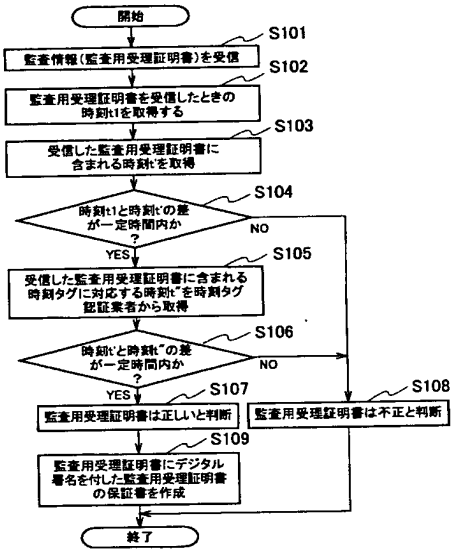
【図２２】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付きハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(r_1, \cdots, r_n)$	
第1次二分木のルート値	H	
2次補完情報	HK2	

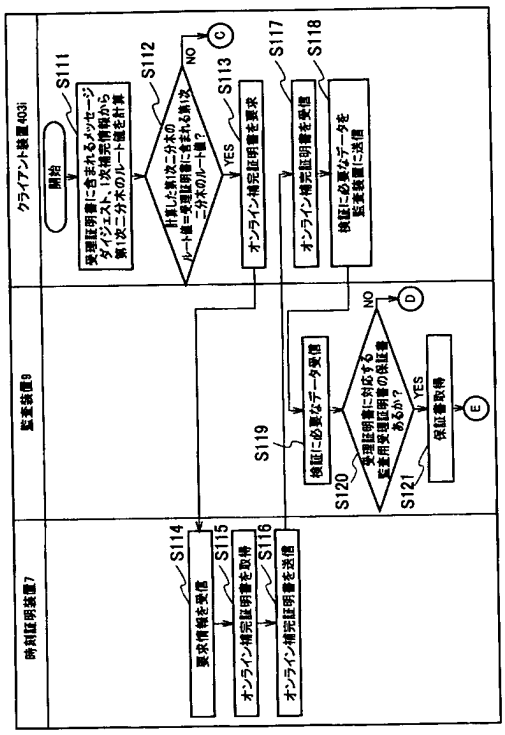
【図２３】



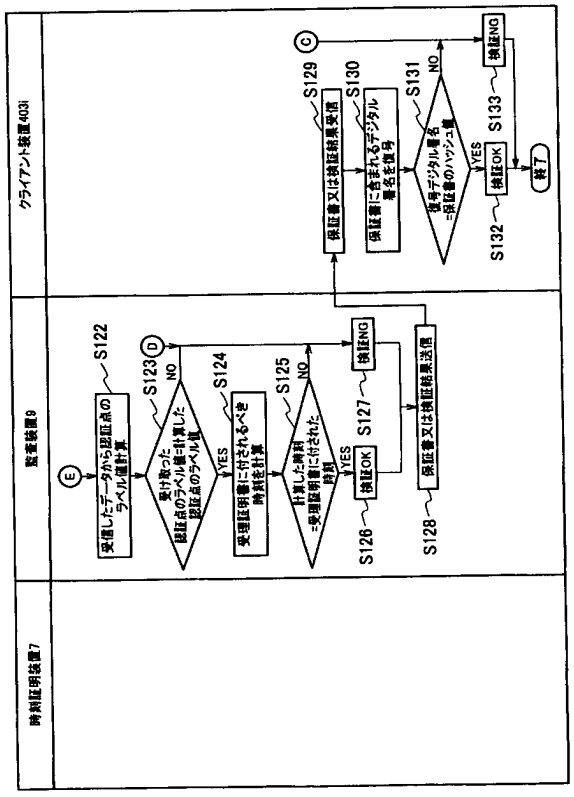
【図２４】



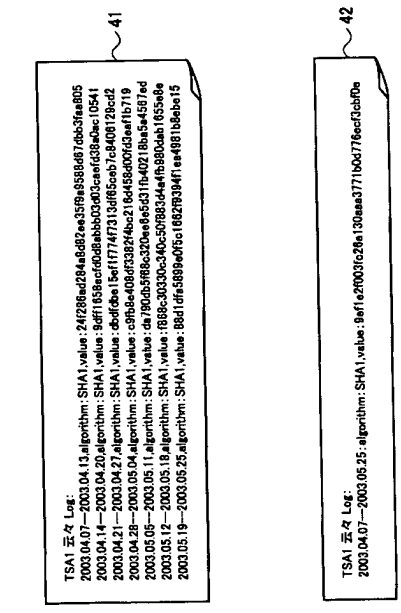
【図２５】



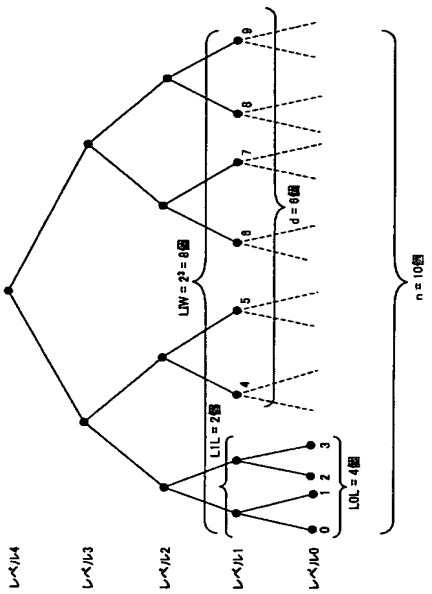
【図２６】



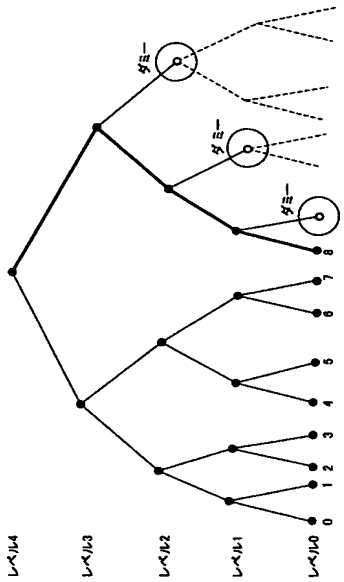
【図２７】



【図２８】



【図２９】

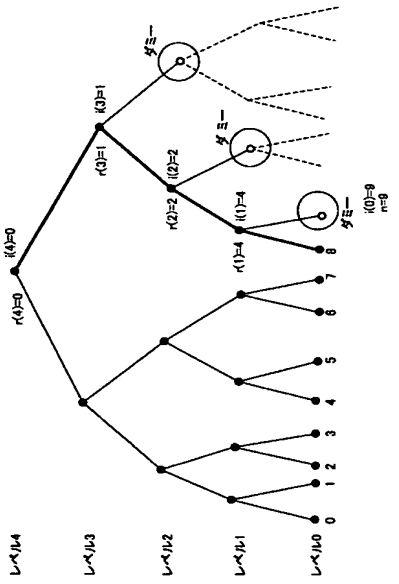


【図３０】

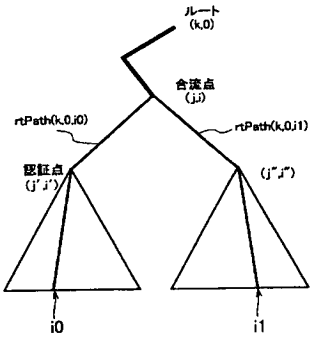
(1)ループ1:定められた時間間隔が終了するまで以下の処理を繰り返す.
(1.1) 受け付けた要求を、変数Xに置く.
(1.2) nを1インクリメントする.
(1.3) ループ2 : j = 0,...,kに対して以下の処理を行う.
(1.3.1) i : = i(j)と置く.
(1.3.2) j = 0のときは、A(0)[i] : = x
(即ち、ノード(j,i(j))にxを設定する).
(1.3.3) j ＞ 0のときは、以下を行う.
・x0 : =A(leftChild(j,i))
(ノード(j,i)のleft−ch::idに割り付けられた値をx0とおく).
・x1 : =A(rightChild(j,i))
(ノード(j,i)のright−childに割り付けられた値をx1とおく).
・x2 : =h(x0 || x1)を計算する.
・A(j)[i] : = x2
(即ち、ノード(j,i)にx2を割り付ける).
(1.3.4) i(j)を1インクリメントする.
(1.3.5) iが偶数のときは、ループ2を抜ける.
ループ2終了.
ループ1終了.
(2)終了時間がきて、ループ1を抜けた後では次の処理を行う.
(2.1) k := ceiling(log2(n))とおく.
(2.2) rtPath(k,0,n−1)を計算し、その結果を(0,r(0)),...,(k,r(k)))と置く.
(2.3) ループ3 : j = 0,...,kに対して以下の処理を行う.
(2.3.1) i : = i(j)とおく.
(2.3.2) j = 0のとき:
(2.3.2.1)iが奇数のとき:
・ダミー値r: = R(0,j)を生成する.
・A(j)[i] : = r
(ノード(0,j)にrを割り当て).
・b(0) : = trueと置く.
・i(0)を1インクリメントする.
(2.3.3) 0 ＜ j ≦ kのとき:
(2.3.3.1): = r(j)のとき
(即ち、ノード(j,i)がrtPath:(k,0,n)上にあるとき):
(2.3.3.1.1)x0 : = A(leftChild(j,i))
(ノード(j,i)のleft−childに割り付けられた値をx0と置く).
(2.3.3.1.2)x1 : = A(rightCh::d(j,i))
(ノード(j,i)のright−childに割り付けられた値をx1と置く).
(2.3.3.1.3)x2 : = h(x0 || x1)を計算する
(2.3.3.1.4)A(j)[i] . = x2
(即ち、ノード(j,i)にx2を割り付ける).
(2.3.3.1.5):iが偶数で、j＜kのとき:
・iを1インクリメントする.
・r : = R(j,i)を計算し、A(j)[i] : = r
(即ち、ノード(j,i)にrを割り当る).
・b(j) : = trueと置く.
・i(j) : = i+1と置く.
(2.3.3.2)i = r(j)+1でiが奇数でj＜kのとき:
・r : = R(j,i)を計算し、A(j)[i] : =r
(即ち、ノード(j,i)にrを割り当てる).
・b(j) : =trueと置く.
・i(j)を1インクリメントする.
ループ3終了.

処理手順1
処理手順2

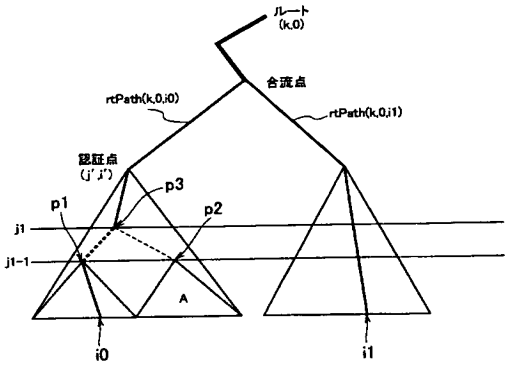
【図３１】



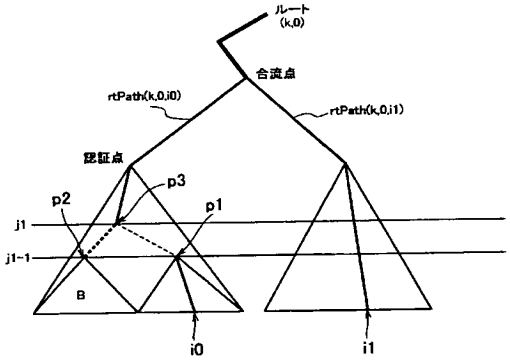
【図３２】



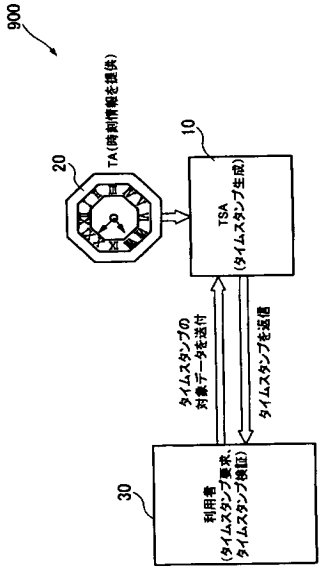
【図３３】



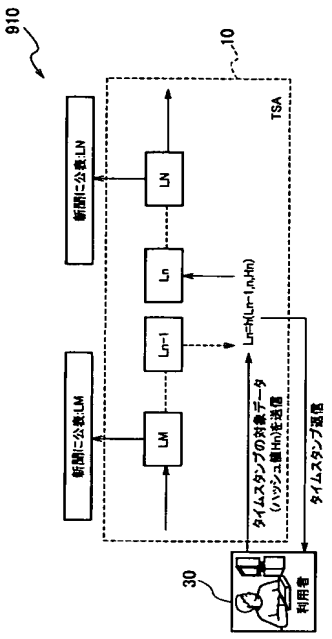
【図３４】



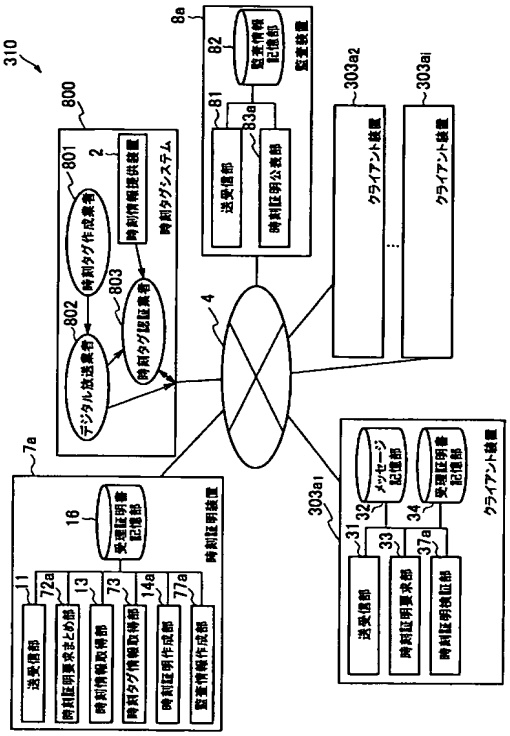
【図３５】



【図３６】



【図３７】



【図３８】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L_h(0,4)),(R_h(1,3)),(L_h(2,0)),(R_h(3,1))]
第1次二分木のルート値	H	

【図３９】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付ハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L_h(0,4)),(R_h(1,3)),(L_h(2,0)),(R_h(3,1))]
第1次二分木のルート値	H	

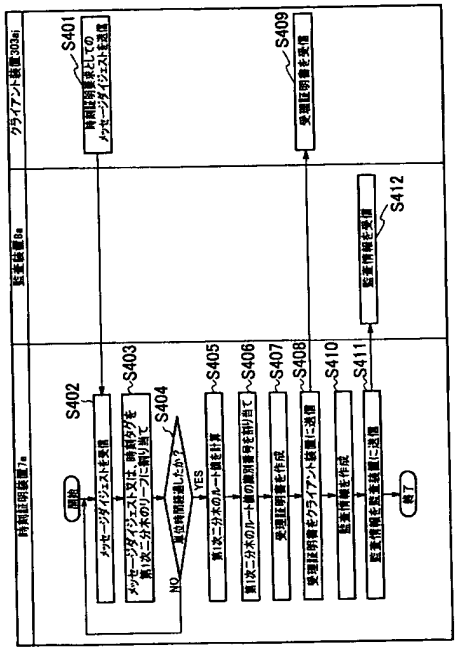
【図４０】

項目	記号	値の例
時刻タグ	τ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L_h(0,4)),(R_h(1,3)),(L_h(2,0)),(R_h(3,1))]
第1次二分木のルート値	H	

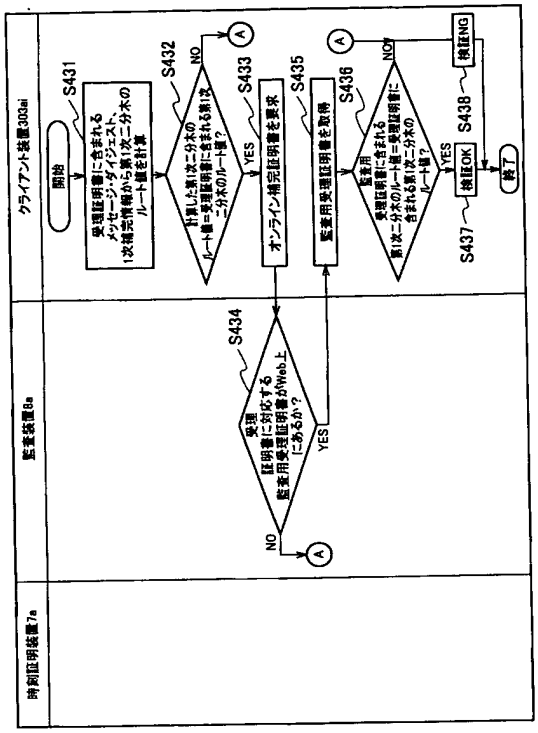
【図４１】

項目	記号	値の例
時刻タグ	τ	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L_h(0,4)),(R_h(1,3)),(L_h(2,0)),(R_h(3,1))]
第1次二分木のルート値	H	

【図４２】



【図４３】



【図４４】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(\tau_1,\cdots,\tau_n)$	
第1次二分木のルート値	H	

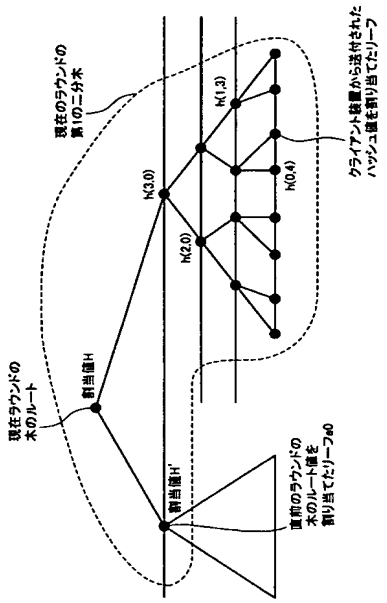
【図４５】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付きハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(\tau_1,\cdots,\tau_n)$	
第1次二分木のルート値	H	

【図４６】

項目	記号	値の例
メッセージ・ダイジェスト	y	
現在のラウンドの終結時刻	t1	
前のラウンドの終結時刻	t2	
第1次二分木のルート値の識別番号		
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(L,H')]
現在のラウンドの第1次二分木のルート値	H	
2次補完情報	HK2	
直前のラウンドの第1次二分木のルート値	H'	
直前のラウンドの第1次二分木のルート値が割り当てられたリーフの1次補完情報	HK1'	[(R,h(3,0)]

【図４７】



【図４８】